Hitachi Gigabit Router GR2000 Series Enhanced Version

Configuration Commands, Vol. 2

GR2K-GA-0014
Ver. 07-02

HITACHI
Inspire the Next

Downloaded from www.Manualslib.com manuals search engine

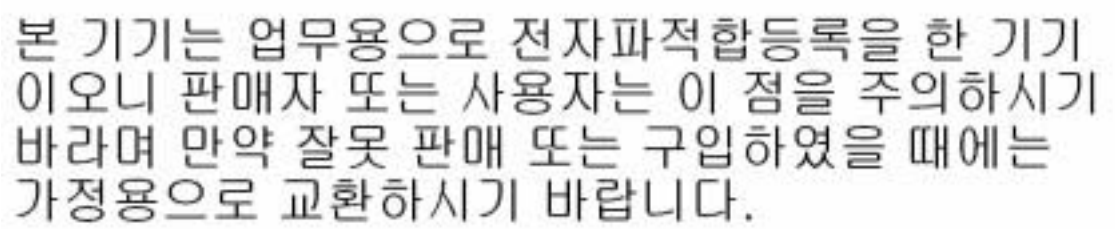
Statement on EN55022 Compliance

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Statement on Federal Communications Commission (FCC) Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense. The user is cautioned that changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Class A Emission Statement (Korea)



Trademarks

Ethernet is a product name of Xerox Corp., USA.
Ethernet is a trademark of Fuji Xerox Co., Ltd.
MS-DOS® is a registered trademark of Microsoft, Corp.
UNIX is a registered trademark, in the USA and other countries, licensed by X/Open Company Limited.
NetWare is a registered trademark of Novell, Inc., USA.
IPX is a registered trademark of Novell, Inc., USA.
HP OpenView is a trademark of Hewlett-Packard Company, USA.
Windows 95 is a trademark of Microsoft, Corp., USA.
Internet Explorer is a registered trademark of Microsoft, Corp., USA.
Netscape Navigator is a registered trademark of Netscape Communications Corporation.
All other brands and product names are trademarks of their respective holders.

Copyright © 2002 Hitachi, Ltd. All Rights Reserved.

Downloaded from www.Manualslib.com manuals search engine

Release 06-05 (December 2002)

This publication contains the most current information available to date. As new and revised sections are received, new updates will be distributed.

Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the expressed written permission of Hitachi, Ltd.

Hitachi, Ltd. reserves the right to make changes to this document at any time without notice, and assumes no responsibility for its use. All the features described in this document may not be currently available.

Change Record

Revision No.	Date	Description	Affected Pages
0	February 2000	Original edition.	—
1	March 2000	Conversion to HICAM format	All
A	July 2000	Edit for Revision A	All
B	August 2000	Edit by ESD	All
C	November 2000	Release 3.00	All
3.02	January 2001	Release 3.02	All
4.00	May 2001	Release 4.00	All
5.00	July 2001	Release 5.00	All
6.01	July 2002	Release 6.01	All
06-05	December 2002	Release 06.05, Reorganized Configuration Guide into three volumes: Settings, Vol. 1, and Vol. 2.	All

Preface

This manual provides a product overview and component details of the GR2000 Gigabit Router Series, and discusses various aspects of product installation, including pre-installation planning, site preparation, unpacking and setup, adding and removing modules, and starting and stopping the router. The manual is intended for personnel involved in the installation and initial setup of the GR2000 Gigabit Router Series. Make sure that you read and understand the Safety section of this manual before beginning installation.

This *GR2000 Configuration Commands, Vol. 2* is one of a set of manuals describing the GR2000 Gigabit Router Series. The table below lists the entire set and provides the full name of the manual. All titles are for version 06-05 unless otherwise noted.

Downloaded from www.Manualslib.com manuals search engine

The information contained in this and other manuals is subject to change without prior notice.

GR2000 Gigabit Router Series Documentation

Title*	Description/Notes	Part Number
Hitachi Gigabit Router GR2000 Series Enhanced Version Applications Guide	In-depth information about the applications and uses for which the router is designed to perform.	GR2K-GA-0001
Hitachi Gigabit Router GR2000 Series Enhanced Version Browser Operations Guide	Operating the GR2000 Gigabit Router Series using the browser interface. This manual is in version 06-03.	GR2K-GA-0005
Hitachi Gigabit Router GR2000 Series Enhanced Version Configuration Settings	The first of three configuration volumes. This manual shows how to create, edit, and manipulate configurations, and provides numerous examples of configurations and appropriate settings.	GR2K-GA-0003
Hitachi Gigabit Router GR2000 Series Enhanced Version Configuration Commands, Vol. 1	This manual provides a configuration command overview, and a complete command reference for router management, network interface, IP information, routing and multicast routing protocols, and MPLS.	GR2K-GA-0013
Hitachi Gigabit Router GR2000 Series Enhanced Version Configuration Commands, Vol. 2	A continuation of volume 1, volume 2 is a command reference for filtering and QoS, IPX and bridge, SNMP, operation management, and a list of all configuration error messages.	GR2K-GA-0014
Hitachi Gigabit Router GR2000 Series Enhanced Version Installation Guide	Provides a product overview and component details of the GR2000 Gigabit Router Series, and discusses various aspects of product installation, including pre-installation planning, site preparation, unpacking and setup, adding and removing modules, and starting and stopping the router.	GR2K-GA-0014
Hitachi Gigabit Router GR2000 Series Enhanced Version Operations - Device Management Overview	This manual is an overview of router operation and includes procedures for starting operation after configuration, using the Command Line Interface (CLI), and commands for daily management, maintenance, and troubleshooting.	GR2K-GA-0015
Hitachi Gigabit Router GR2000 Series Enhanced Version Operations Commands, Vol. 1	This is volume 1 of 2 volumes of operation commands. This manual is used for “new syntax” commands only. For the original GR2000 UNIX-based command-line interface, see the *GR2000 Operations Guide, UNIX-Based Interface*, below.	GR2K-GA-0016
Hitachi Gigabit Router GR2000 Series Enhanced Version Operations Commands, Vol. 2	This is volume 2 of 2 volumes of operation commands. This manual is used for “new syntax” commands only. For the original GR2000 UNIX-based command-line interface, see the *GR2000 Operations Guide, UNIX-Based Interface*, below.	GR2K-GA-0017
Hitachi Gigabit Router GR2000 Series Enhanced Version Operations Log and MIB Reference	This operation manual presents a list of LED display and fault codes, maintenance information, operation and log messages, and complete MIB descriptions.	GR2K-GA-0018
Hitachi Gigabit Router GR2000 Series Enhanced Version Operations Guide, UNIX-Based Interface	Operating the GR2000 Gigabit Router Series using the original UNIX-based command-line interface. This manual is in version 06-03.	GR2K-GA-0004
Hitachi Gigabit Router GR2000 Series Enhanced Version Maintenance Guide	Provides and introduction to maintenance, troubleshooting flowcharts and checklists, and hardware information, such as voltage checks and parts replacement procedures.	GR2K-ZG-1001

Downloaded from www.Manualslib.com manuals search engine

GR2000 Gigabit Router Series Documentation (continued)

Hitachi Gigabit Router GR2000 Series Enhanced Version Quick Start Guide	The purpose of the Quick Start Guide is to provide a concise guide to setting up the GR2000. It includes a guide to the documentation set, roadmaps, and instructions for performing the most common configuration and operations procedures.	GR2K-GA-0006
Hitachi Gigabit Router GR2000 Series Enhanced Version Safety Guide	This guide discusses general and specific safety instructions regarding the *GR2000 Gigabit Router Series*. This guide is also available in German.	GR2K-GA-0009 GR2K-GA-0009G
* *When used in the documentation, the manual title is almost always shortened to, for example,* GR2000 Configuration Commands, Vol. 1.		

Abbreviations

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
AC	Access Concentrator
ADSL	Asymmetric Digital Subscriber line
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
AFI	Authority and Format Indicator
AIS	Alarm Indication Signal
ALG	Application Level Gateway
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AUX	Auxiliary
BAP	Bandwidth Allocation Protocol
BAS	Broadband Access Server
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - Version 4
bit/s	bits per second, usually abbreviated bps.
BOD	Bandwidth On Demand
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface

Downloaded from www.Manualslib.com manuals search engine

BSR	Boot Strap Router
CATV	Cable Television
CBR	Constant Bit Rate
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CLLM	Consolidated Link Layer Management
CLNP	Connectionless Network Protocol
CLP	Cell Loss Priority
CNTL	CoNTrol
COPS	Common Open Policy Service
CoS	Class of Service
CRC	Cyclic Redundancy Check
CR-LDP	Constraint-Based Label Distribution Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DCC	Data Country Code
DCE	Data Circuit terminating Equipment
DDP	Datagram Delivery Protocol
DHCP	Dynamic Host Configuration Protocol
Diff-serv	Differentiated Services
DLCI	Data Link Connection Identifier
DLSw	Data Link Switch
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSP	Domain Specific Part
DSU	Digital Service Unit
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
ELAN	Emulated LAN
E-Mail	Electronic Mail
EoMPLS	Ethernet over MPLS
ERP	Echo Response
ERQ	Echo Request
ES	End System

Downloaded from www.Manualslib.com manuals search engine

FCS	Frame Check Sequence
FDB	Filtering Data Base
FDDI	Fiber Distributed Data Interface
FEC	Forwarding Equivalence Class
FECN	Forward Explicit Congestion Notification
FERF	Far End Receive Failure
FQDN	Fully Qualified Domain Name
FR	Frame Relay
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GFR	Guaranteed Frame Rate
HDLC	High-level Data Link Control
HNA	Hitachi Network Architectural
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IDI	Initial Domain Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
ILMI	Interim Local Management Interface
INS	Information Network System
IP	Internet Protocol
IPsec	Security Architecture for IP
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication, Standardization Sector
JDI	Japanese Domain Identifier
L2-VPN	Layer 2 - Virtual Private Network

Downloaded from www.Manualslib.com manuals search engine

LAN	Local Area Network
LAPB	Link Access Procedure Balanced Mode
LCP	Link Control Protocol
LDP	Label Distribution Protocol
LEC	LAN Emulation Client
LED	Light Emitting Diode
LES	LAN Emulation Server
LIS	Logical IP Subnetwork
LLB	Local Loop Back
LLC	Logical Link Control
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LQM	Link Quality Monitoring
LQR	Link Quality Report
LSP	Label Switched Path
LSR	Label Switched Router
MAC	Media Access Control
MC	Memory Card
MCR	Media Access Control
MD5	Message Digest 5
MIB	Management Information Base
MLD	Multicast Listener Discovery
MMF	Multi Mode Fiber
MPLS	Multi-Protocol Label Switching
MRU	Maximum Receive Unit
MSS	Maximum Segment Size
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAPT	Network Address Port Translation
NAPT-PT	Network Address Port Translation - Protocol Translation
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
NBP	Name Binding Protocol
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NetBIOS	Network Basic Input/Output System

Downloaded from www.Manualslib.com manuals search engine

NIF	Network Interface board
NLA ID	Next-Level Aggregation Identifier
NLP	Network Layer Protocol
NRZ	Non-Return-to-Zero
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operation Administration and Management
OC-3c	Optical Carrier level 3 concatenation
OC-12c	Optical Carrier level 12 concatenation
OC-48c	Optical Carrier level 48 concatenation
ONU	Optical Network Unit
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	Packets Per Second, sometimes abbreviated as pps
PAD	PADding
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-confirmation
PADT	PPPoE Active Discovery Terminate
PC	Personal Computer
PCR	Peak Cell Rate
PDB	Permanent Data Base
PDU	Protocol Data Unit
PHY	PHYsical layer protocol
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PLD	Programmable Logic Design
POS	PPP over SONET/SDH
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet

Downloaded from www.Manualslib.com manuals search engine

PRI	Primary Rate Interface
PSS	Product Support Service
PVC	Permanent Virtual Channel (Connection)/Permanent Virtual Circuit
QoS	Quality of Service
RA	Router Advertisement
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RLB	Remote Loop Back
RM	Routing Manager
RMON	Remote Network Monitoring MIB
RP	Routing Processor
RPF	Reverse Path Forwarding
RQ	ReQuest
RSVP	Resource Reservation Protocol
SA	Source Address
SAP	Service Access Point
SD	Start Delimiter
SDH	Synchronous Digital Hierarchy
SD-I	Super Digital I interface
SDLC	Service Advertising Protocol
SDU	Service Data Unit
SFD	Start Frame Delimiter
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNA	Systems Networking Architecture
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPF	Shortest Path First
SPT	Spanning Tree
SPX	Sequenced Packet Exchange
SSAP	Source Service Access Point

Downloaded from www.Manualslib.com manuals search engine

SSP	Switch to Switch Protocol
SST	System Simulation Test
SVC	Switched Virtual Channel (Connection)
TA	Terminal Adapter
TCC	Transmission Control Character
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTC	Telecommunication Technology Committee
TTL	Time To Live
UBR	Unspecified Bit Rate
UBR+	Unspecified Bit Rate plus
UDP	User Datagram Protocol
UNI	User Network Interface
UPC	Usage Parameter Control
VBR	Variable Bit Rate
VC	Virtual Channel/Virtual Call
VCI	Virtual Channel Identifier
VLAN	Virtual LAN
VoIP	Voice over IP
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
WS	Work Station
WWW	World Wide Web
xDSL	x Digital Subscriber Line

Downloaded from www.Manualslib.com manuals search engine

Acknowledgments

[GateD]

Copyright © 1995, 1996, 1997, 1998 The Regents of the University of Michigan. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators.

[SNMP]

****

Copyright 1988-1996 by Carnegie Mellon University. All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.

****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.

****

Some of this software is Copyright © 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty.

****

* Primary Author: Steve Waldbusser

Downloaded from www.Manualslib.com manuals search engine

* Additional Contributors:

Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.

David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC

Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application was adopted by David Waitzman

Many more over the years...

[BSDI Internet Server]

BERKELEY SOFTWARE DESIGN, INC.

Copyright © 1992, 1993, 1994, 1995, 1996, 1997 Berkeley Software Design, Inc.

This product includes BSDI Internet Server developed by Berkeley Software Design, Inc.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must also play the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND

Downloaded from www.Manualslib.com manuals search engine

ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase “this text” refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase “This material” refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

Contributors: Sun Microsystems, Inc., Keith Muller, Mark Nudelman, Jan-Simon Pendry

AT&T (DAVID M. GAY)

Copyright © 1991 by AT&T. Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED “AS IS”, WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

Downloaded from www.Manualslib.com manuals search engine

INFO-ZIP GROUP

This product includes Info-ZIP's software which is used for a part of the boot program. Info-ZIP's software (ZIP, UnZip and related utilities) is free and can be obtained as source code or executables from various bulletin board services and anonymous-ftp sites, including CompuServe's IBMPRO forum and ftp.uu.net:/pub/archiving/zip/*.

INTERNET SOFTWARE CONSORTIUM

Copyright © 1996 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

SIGMASOFT, TH. LOCKERT

Copyright © 1994 SigmaSoft, Th. Lockert <tholo@sigmasoft.com> All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Downloaded from www.Manualslib.com manuals search engine

SUN MICROSYSTEMS, INC.

Copyright © 1984, 1985, 1986, 1987, 1988, 1993 Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California 94043

UNIVERSITY OF TORONTO

Copyright © 1986 by University of Toronto. Written by Henry Spencer. Not derived from licensed software. Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

WASHINGTON UNIVERSITY IN SAINT LOUIS

Copyright © 1993, 1994 Washington University in Saint Louis All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following

Downloaded from www.Manualslib.com manuals search engine

acknowledgement: This product includes software developed by the Washington University in Saint Louis and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY WASHINGTON UNIVERSITY AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL WASHINGTON UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WILDBOAR

Portions or all of this file are Copyright © 1994,1995,1996 Yoichi Shinoda, Yoshitaka Tokugawa, WIDE Project, Wildboar Project and Foretune. All rights reserved. This code has been contributed to Berkeley Software Design, Inc. by the Wildboar Project and its contributors. The Berkeley Software Design Inc. software License Agreement specifies the terms and conditions for redistribution.

THIS SOFTWARE IS PROVIDED BY THE WILDBOAR PROJECT AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WILDBOAR PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MARTIN BIRGMEIER

Copyright © 1993 Martin Birgmeier. All rights reserved. You may redistribute unmodified or modified versions of this source code provided that the above copyright notice and this and the following conditions are retained.

This software is provided “as is”, and comes with no warranties of any kind. I shall in no event be liable for anything that happens to anyone/anything when using this software.

CHRISTOPHER G. DEMETRIOU

Copyright © 1993, 1994 Christopher G. Demetriou. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Christopher G. Demetriou.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DAVID HOVEMEYER

Copyright © 1995 David Hovemeyer <daveho@infocom.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE DEVELOPERS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE DEVELOPERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FRANK VAN DER LINDEN

Copyright © 1995 Frank van der Linden. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed for the NetBSD Project by Frank van der Linden
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THEO DE RAADT

Copyright © 1992/3 Theo de Raadt <deraadt@fsa.ca>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HENRY SPENCER

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

[diff, grep]

Copyright © 1988, 1989, 1992, 1993, 1994 Free Software Foundation, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

[less]

Copyright © 1984,1985,1989,1994,1995,1996 Mark Nudelman All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

Downloaded from www.Manualslib.com manuals search engine

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tcpd]

Copyright 1995 by Wietse Venema. All rights reserved. Some individual files may be covered by other copyrights.

This material was originally written and compiled by Wietse Venema at Eindhoven University of Technology, The Netherlands, in 1990, 1991, 1992, 1993, 1994 and 1995.

Redistribution and use in source and binary forms are permitted provided that this entire copyright notice is duplicated in all such copies.

This software is provided “as is” and without any expressed or implied warranties, including, without limitation, the implied warranties of merchantibility and fitness for any particular purpose.

[tcpdump]

Copyright © 1989 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright © 1990, 1991, 1993, 1994 John Robert LoVerso. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by John Robert LoVerso.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This implementation has been influenced by the CMU SNMP release, by Steve Waldbusser. However, this shares no code with that system. Additional ASN.1 insight gained from Marshall T. Rose's _The_Open_Book_. Earlier forms of this implementation were derived and/or inspired by an awk script originally written by C. Philip Wood of LANL (but later heavily modified by John Robert LoVerso). The copyright notice for that work is preserved below, even though it may not rightly apply to this file.

Downloaded from www.Manualslib.com manuals search engine

This started out as a very simple program, but the incremental decoding (into the BE structure) complicated things.

Los Alamos National Laboratory

Copyright, 1990. The Regents of the University of California. This software was produced under a U.S. Government contract (W-7405-ENG-36) by Los Alamos National Laboratory, which is operated by the University of California for the U.S. Department of Energy. The U.S. Government is licensed to use, reproduce, and distribute this software. Permission is granted to the public to copy and use this software without charge, provided that this Notice and any statement of authorship are reproduced on all copies. Neither the Government nor the University makes any warranty, express or implied, or assumes any liability or responsibility for the use of this software.

[traceroute]

Copyright © 1988, 1989, 1991, 1994, 1995, 1996 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: “This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.” Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[zlib]

Copyright notice: © 1995-1996 Jean-loup Gailly and Mark Adler

This software is provided “as-is”, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

Downloaded from www.Manualslib.com manuals search engine

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
gzip@prep.ai.mit.edu madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

[Apache HTTP server]

Copyright © 1995-1998 The Apache Group. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).”

4. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called “Apache” nor may “Apache” appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the Apache Group for use in the Apache HTTP server project (http:// www.apache.org/).”

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

Downloaded from www.Manualslib.com manuals search engine

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[Xntp Program]

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright © David L. Mills 1992, 1993, 1994, 1995, 1996 Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[MD5 Program]

Adapted from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

[pimdd]

Copyright © 1998 by the University of Oregon. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Oregon. The name of the University of Oregon may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF OREGON DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL UO, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Downloaded from www.Manualslib.com manuals search engine

Questions concerning this software should be directed to Kurt Windisch (kurtw@antc.uoregon.edu)

$Id: LICENSE,v 1.2 1998/05/29 21:58:19 kurtw Exp $

Part of this program has been derived from PIM sparse-mode pimd. The pimd program is covered by the license in the accompanying file named "LICENSE.pimd".

The pimd program is COPYRIGHT 1998 by University of Southern California.

Part of this program has been derived from mrouted. The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[mrouted]

The mrouted program is covered by the following license. Use of the mrouted program represents acceptance of these terms and conditions.

1. STANFORD grants to LICENSEE a nonexclusive and nontransferable license to use, copy and modify the computer software "mrouted" (hereinafter called the "Program"), upon the terms and conditions hereinafter set out and until Licensee discontinues use of the Licensed Program.

2. LICENSEE acknowledges that the Program is a research tool still in the development state, that it is being supplied "as is," without any accompanying services from STANFORD, and that this license is entered into in order to encourage scientific collaboration aimed at further development and application of the Program.

3. LICENSEE may copy the Program and may sublicense others to use object code copies of the Program or any derivative version of the Program. All copies must contain all copyright and other proprietary notices found in the Program as provided by STANFORD. Title to copyright to the Program remains with STANFORD.

4. LICENSEE may create derivative versions of the Program. LICENSEE hereby grants STANFORD a royalty-free license to use, copy, modify, distribute and sublicense any such derivative works. At the time LICENSEE provides a copy of a derivative version of the Program to a third party, LICENSEE shall provide STANFORD with one copy of the source code of the derivative version at no charge to STANFORD.

5. STANFORD MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, STANFORD MAKES NO REPRESENTATION OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PROGRAM WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. STANFORD shall not be held liable for any liability nor for any direct, indirect or consequential damages with respect to any claim by LICENSEE or any third party on account of or arising from this Agreement or use of the Program.

6. This agreement shall be construed, interpreted and applied in accordance with the State of California and any legal action arising out of this Agreement or use of the Program shall be filed in a court in the State of California.

Downloaded from www.Manualslib.com manuals search engine

7. Nothing in this Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise any trademark or the name of ‘‘Stanford’’.

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[PIM sparse-mode pimd]

Copyright © 1998 by the University of Southern California. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute. The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF SOUTHERN CALIFORNIA DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL USC, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Pavlin Ivanov Radoslavov (pavlin@catarina.usc.edu)

$Id: LICENSE.pimd,v 1.1 1998/05/29 21:58:20 kurtw Exp $

Part of this program has been derived from mrouted. The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[KATE IPv6 STACK]

Copyright O 1995,1996,1997,1998 and 2000 by WIDE Project.All rights reserved reserved.

Redistribution and use in source and binary forms,with or without modification,are permitted provided that the following conditions are met:

Downloaded from www.Manualslib.com manuals search engine

1.Redistributions of source code must retain the above copyright notice,this list of conditions and the following discllaimer

2.Redistributions in binary form must reproduce the above copyrigt notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.Neither the name of the projecct nor the names of its contributors may be used to endorse or promote products derived from thissoftware without specific prior written permissions.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ”AS IS”AND ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO,THE IMPLIED WARRANTIES OF MERCHANTABILITY AND AND FITNESS FOR A PATICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,INDIRECT,INCIDENTAL,SPECIAL,EXEMPLARY,OR CONSEQUENTIAL DAMAGED (INCLUDING,BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES ; LOSS OF USE,DATA,OR PROFITS;OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,WHETHER IN CONTRACT,STRICT LIABILITY,OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGEDÅD

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Safety Guide

This document provides safety-related notices for use of the GR2000 Gigabit Router. Read the following Safety Guidelines carefully before using the product and follow them to take full advantage of the GR2000's features.

General Safety Guidelines

- Perform all operations in accordance with the instructions and procedures as described in the product manuals.
- Be alert and use common sense. The hazard warnings cannot cover every possible situation. Do not perform any operations not described in the documentation. In the event of a problem, turn off the power, unplug the power cable, and contact a qualified service technician.
- Follow all precautionary and hazard messages on the GR2000 and in the documentation. Failure to do so may result in bodily injury, damage to the device, or an interruption in service.
- The hazard warnings on the machine or in the manual have the following headings and symbols, CAUTION or WARNING. Hazard warnings on the device and in the manuals are provided to prevent or reduce risk of death, personal injury, or product damage. Understand and follow these hazard warnings:

Caution: **This is a caution notice. Follow the instructions in this notice to avoid damage to the equipment or a disruption in service.**

DANGER: **This is a warning notice. Follow the instructions in this notice to avoid the possibility of bodily injury occurring.**

The following sections have specific instructions regarding warnings and cautions.

Downloaded from www.Manualslib.com manuals search engine

Specific Warning Instructions

DANGER: Failure to follow the instructions in this section could cause bodily injury or death to the user.

- Do not operate the device if you suspect damage or failure.
- Do not use the device if there is smoke or an unusual smell coming from the system. If either occurs, immediately turn power off and unplug the power cable from the outlet. Contact a qualified service technician.
- In the case of the GR2000-20H, GR2000-10H, or GR2000-6H with DC power supplies installed, turn off the circuit breaker on the power facility supply side.
- If the device is installed in a rack, unplug the device power cable from the rack outlet. If the component with the problem cannot be identified, remove all power cables from the rack outlet. Contact a qualified service technician.
- In the case of redundant power supplies, make sure that ALL switches and circuit breakers are turned off.
- If the device is dropped and any part is broken, turn the power switch off, unplug the power cable from the outlet, and contact service. Continued use may cause fire or electric shock.
- Do not use any unspecified power source or power voltage. Observe all terminal ratings and markings on the product.
- To prevent electric shock, use only grounded power outlets when using AC power. Do not overload power outlets. In the case of DC power or the GR2000-20H, use a ground wire to prevent electric shock.
- Do not use adapters to connect multiple power cables to the same outlet. Use standard safety procedures with the power cable.
- Use only the power cable supplied with the device. Use of other cables may cause fire or electric shock. Keep the power cable away from extreme heat.
- Similarly, do not use the provided power cable for products other than the GR2000, since this could cause a fire or electrical shock hazard.
- Do not operate the device in wet or damp conditions
- If liquid is spilled on the device, turn power off and unplug the power cable from the outlet. Discontinue use to avoid the risk of fire or electric shock.
- Place device on a stable, level surface. Do not place or stack objects on top of the device.
- If a foreign object falls into the device, turn power off and unplug the power cable from the outlet. Do not attempt to remove the object while the power is on.
- Do not remove the device's cover while the device is in operation.
- Touching internal parts may cause electric shock. Contact a qualified service technician for any internal inspection, adjustment or repair. Do not modify the device. Doing so may cause fire or electric shock.
- Do not insert any foreign objects into the device or the ventilation slots. Doing so may cause fire or electric shock.
- Do not insert hands or any other object into a fan.
- Do not allow unauthorized users of the device to pull out boards or power supplies at any time.
- Do not set the GR2000 in a dusty or humid location. Doing so may cause fire or electric shock.

Downloaded from www.Manualslib.com manuals search engine

- This router contains a lithium battery for the real-time clock. Mishandling this battery may cause heat build-up, damage, or in an extreme case, explosion or fire.
  - Do not remove the battery from the device, disassemble it, or expose it to temperatures of over 100°C (212°F)
  - Do not throw or immerse lithium batteries into water.
  - Dispose of exhausted batteries as required by local regulations.
- Remove dust on and around the device regularly. Dust buildup can cause fire or electrical shock, and can result in failure of the device.
- The power supply of the GR2000-6H weighs 8 kg. Handle with care, since it could cause injury if it is dropped.

Specific Caution Instructions

Caution: **This is a caution notice. Follow the instructions in this notice to avoid damage to the equipment or a disruption in service.**

- Condensation may form on the surface and inside the device if it is moved from a cold to a warm location. Using the device in this condition may cause fire or electric shock. After moving the device between two locations with a large temperature variation, let the device stand for a few hours before using.
- Do not block the device's ventilation.
- Move the device carefully. Before moving the device, unplug the power cable, disconnect all exterior devices, and remove the stabilization clamps. Failure to follow this warning may damage the device or power cable, causing fire or electric shock.
- Do not hold the device by the front and back when moving; the cover may come off, causing the device to fall.
- Do not subject the device to extreme temperatures.
- Do not place the device in direct sunlight or near heat sources that may cause damage.
- A yellow label designates that a Class 1 laser is being used. Light emission is minimal and not hazardous, but avoid looking directly into the laser beam.
- Approximate weights of the GR2000 models are as follows:
  - GR2000-2S: Approx. 15 kg. (33 lbs.)
  - GR2000-4S: Approx. 21 kg. (46 lbs.)
  - GR2000-6H: Approx. 55 kg. (121 lbs.)
  - GR2000-10H: Approx. 120 kg. (264 lbs.)
  - GR2000-20H: Approx. 160 kg. (352 lbs.)

Downloaded from www.Manualslib.com manuals search engine

Other Instructions

Cleaning

- Clean the device only with a clean, dry cloth or use a cloth that has been dampened with water or another pH-neutral liquid and thoroughly wrung out.
- Do not use volatile organic solutions such as benzene or paint thinner, chemicals, chemically treated cloths or pesticides, which may deform, discolor or damage the device.

Storage

Unplug the power cable from the outlet when the device is not used for long periods.

For users in the UK and Denmark

This is Class I Equipment. In the UK and Denmark, set up this equipment as Pluggable Equipment Type B and connect to the equipment grounding point with a grounded plug.

Downloaded from www.Manualslib.com manuals search engine

Table of Contents

Chapter 1 - Filtering/QoS Information 1-1

1.1 Flow Information 1-2
1.1.1 IPv4 Flow Control 1-2
1.1.2 IPv6 Flow Control 1-6
1.1.3 flow (Flow Information) 1-9
1.1.4 flow filter (Filter Flow Information) 1-24
1.1.5 flow filter (IPv4) 1-26
1.1.6 flow filter (IPv6) [ROUTE-OS6] 1-43
1.1.7 flow qos (QoS Flow Information) 1-57
1.1.8 flow qos (IPv4) 1-58
1.1.9 flow qos (IPv6) [ROUTE-OS6] 1-83
1.1.10 filter 1-108
1.1.11 filter-list (Filter List Information in the Old BSD UNIX-Based Command System) 1-110
1.1.12 filter-group (Information on Filter Group of Old BSD UNIX-Based Command System) 1-124
1.1.13 filter-interface (Information on Filter Interface of Old BSD UNIX-Based Command System) 1-128

1.2 Quality of Service (QoS) Objects 1-131
1.2.1 qos 1-134
1.2.2 qos-queue-list 1-138
1.2.3 qos-interface 1-153
1.2.4 qos-discard-mode 1-166
1.2.5 qos-ip-list (Information on QoS IP Frame Condition of the Old BSD UNIX-Based Command System) 1-168
1.2.6 qos-ip-list-group (Information on QoS IP Frame Condition Group of the Old BSD UNIX-based Command System) 1-194
1.2.7 qos-tos-map 1-196
1.2.8 qos-ip (Information on IP QoS of the Old BSD UNIX-based Command System) 1-201
1.2.9 qos-ipx 1-205
1.2.10 qos-bridge 1-207
1.2.11 qos-hdlc-passthrough 1-209
1.2.12 shaper (shaper transmission information) 1-212

1.3 COPS 1-218
1.3.1 COPS 1-218

Chapter 2 - IPX/Bridge Information 2-1

2.1 IPX Objects 2-1
2.1.1 ipx 2-1

Downloaded from www.Manualslib.com manuals search engine

2.1.2 ipx-interface 2-3
2.1.3 ipx-arp 2-9
2.1.4 static-route 2-11
2.1.5 static-sap 2-14
2.1.6 rip-filtering 2-18
2.1.7 sap-filtering 2-21
2.1.8 ipx-filtering 2-24
2.2 Bridge Objects 2-29
2.2.1 bridge 2-29
2.2.2 bridge-interface 2-30
2.2.3 filtering-database 2-33
2.2.4 extended-filtering 2-35
2.2.5 spanning-tree 2-39

Chapter 3 - SNMP Information 3-1

3.1 SNMP Objects 3-1
3.1.1 snmp 3-1
3.1.2 history-control 3-8
3.1.3 alarm 3-12
3.1.4 event 3-19

Chapter 4 - Operation Management Information 4-1

4.1 Host Name Information 4-1
4.1.1 hosts 4-1
4.1.2 dns-resolver 4-3
4.2 Log Information 4-7
4.2.1 logger-syslog 4-7
4.2.2 logger-email 4-9
4.2.3 logger-email-from (Log E-Mail Transmission Source Information) 4-11
4.2.4 logger-smtp 4-12
4.3 report (e-mail report information) 4-15
4.4 NTP Object - ntp 4-20
4.5 radius (RADIUS server information) 4-27
4.6 Board Disablement Object - disable 4-31
4.7 Default Configuration Objects 4-33
4.7.1 default 4-33
4.7.2 SNMP Information 4-34
4.7.3 Line Information (Ethernet/Gibabit Ethernet) 4-35
4.7.4 Line Information (WAN) 4-36
4.7.5 Line Information (WAN OC-POS) 4-38
4.7.6 line Information (ATM) 4-40
4.7.7 Subline Information (WAN) 4-41

Downloaded from www.Manualslib.com manuals search engine

4.7.8 PPP Information 4-42
4.7.9 PPPoE Information 4-43
4.7.10 Frame Relay Information 4-44
4.7.11 ATM Information 4-46
4.7.12 ISDN Information (Japan Only) 4-48
4.7.13 Tunnel Interface Information 4-50
4.7.14 IP Interface Information 4-51
4.7.15 NAT-PT Information 4-53
4.7.16 IPX Information 4-54
4.7.17 Bridge information 4-56
4.7.18 QoS Information 4-57
4.7.19 Filter Information 4-59
4.7.20 router-default 4-60

Chapter 5 - Configuration Error Messages 5-1

5.1 Common 5-2
5.2 Router Control Information 5-3
5.3 Network Interface 5-4
5.4 IP Information 5-14
5.5 Routing Protocol 5-20
5.6 Multicast Routing Protocol 5-52
5.7 IPv6 Multicast Routing Protocol 5-62
5.8 Flow Information Error Messages 5-64
5.9 Filter and QoS Information (Other than Flow Information) 5-76
5.10 MPLS Information 5-83
5.11 IPX Information 5-88
5.12 Bridge Information 5-91
5.13 VRRP Information 5-92
5.14 SNMP Information 5-93
5.15 COPS Information 5-94
5.16 RADIUS 5-95
5.17 Operation Management Information 5-96
5.18 Address Translation Information 5-97
5.19 DHCP Server Information 5-99
5.20 DHCP Client Information 5-100
5.21 NAT-PT 5-100
5.22 DNS Resolver Information 5-101
5.23 Log Information 5-101
5.24 E-Mail Sending Information 5-101
5.25 Other Error Messages 5-102

Downloaded from www.Manualslib.com manuals search engine

Index Index-1

Downloaded from www.Manualslib.com manuals search engine

List of Figures

Chapter 1 - Filtering/QoS Information 1-1

Figure 1-1. Range of QoS, Filter-Flow Control 1-2
Figure 1-2. Control Range for QoS Queue Attribute and QoS Interface Information 1-4
Figure 1-3. Control Range for QoS Discard Mode 1-5
Figure 1-4. Control Range of QoS Information..... 1-131
Figure 1-5. Range of QoS Attribute and Qos Interface Control 1-131
Figure 1-6. Range of QoS Discard Mode Control..... 1-132
Figure 1-7. Range of QoS IP Frame Condition Information, QoS IP Frame Condition Group Information, and IP QoS Information Control..... 1-133
Figure 1-8. Range of TOS-QoS Conversion Table Information Control..... 1-134
Figure 1-9. Maximum Band Limitation + Minimum Band Guarantee..... 1-177
Figure 1-10. Maximum Band Limitation + Important Packet Protection 1-178
Figure 1-11. Maximum Band Limitation + Minimum Band Guarantee + Important Packet Protection 1-178
Figure 1-12. Effect of QoS Configuration Definition Output Priority in ATM Line 1-204

Chapter 2 - IPX/Bridge Information.....2-1

Chapter 3 - SNMP Information 3-1

Chapter 4 - Operation Management Information.....4-1

Chapter 5 - Configuration Error Messages 5-1

Index Index-1

Downloaded from www.Manualslib.com manuals search engine

This page left intentionally blank

Downloaded from www.Manualslib.com manuals search engine

List of Tables

Chapter 1 - Filtering/QoS Information 1-1

Table 1-1. Features of Each Constituting Definition Inputting Form for Filter Flow Information.. 1-5
Table 1-2. Feature of Constituting Definition of QoS Flow Information by Each Input Form..... 1-6
Table 1-3. Features of Each Constituting Definition Inputting Form for *flow filter* Information.... 1-7
Table 1-4. Features of Each Constituting Definition Inputting Form for *flow qos* Information 1-7
Table 1-5. List of Interfaces that Support Flow Control 1-8
Table 1-6. Types of action that have an affect when using filter flow information and QoS flow information in combination 1-9
Table 1-7. Supported L2 UPC functions for each RP type 1-11
Table 1-8. Priority for Each Packet Type When *classify_all_off* is Specified (All Models Except GR2000-1B and GR2000-2B) 1-12
Table 1-9. Priority for Each Packet Type When *classify_all* is Specified (All Models Except GR2000-1B, GR2000-2B and GR2000-2B+)..... 1-13
Table 1-10. Priority for Each Packet Type When *classify_all_off* is Specified (For all Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control)..... 1-14
Table 1-11. Priority for Each Packet Type When *classify_all_off* is Specified (All Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control) 1-15
Table 1-12. Priority for Each Packet Type When *classify_all* is Specified (All Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control) 1-16
Table 1-13. Priority for Each Packet Type When *classify_all* is Specified (All Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control) 1-17
Table 1-14. Priority for Each Packet Type When -classify_all_off is Specified (GR2000-BH)..... 1-18
Table 1-15. Priority for Each Packet Type When -classify_all is Specified (GR2000-BH) 1-19
Table 1-16. Priority for Each Packet Type When -classify_all_off is Specified (NE1G-2D)..... 1-20
Table 1-17. Priority for Each Packet Type When -classify_all is Specified (NE1G-2D) 1-21
Table 1-18. Relationship between user priority and send queue number..... 1-21
Table 1-19. Relay Performance When Setting the *flow filter* and *flow qos* Commands (Semi-Duplication Communication) 1-24
Table 1-20. Maximum Definable Entries by Each PM Mounting Memory Size 1-25
Table 1-21. List of Parameters that Can Be Set for Each RP Type Using IPv4 Filter Flow Information 1-28
Table 1-22. General Protocol Number..... 1-30
Table 1-23. Relationship between Upper and Lower IP User Data Length Llimits and IP User Data Length..... 1-31
Table 1-24. General port number..... 1-32
Table 1-25. General ICMP Type and Code Nnumber..... 1-33
Table 1-26. General ICMP Type Number 1-33
Table 1-27. List of Interfaces Supporting Flow Control..... 1-34
Table 1-28. Packet Type in which the Filtering Based on the Flag (ACK and SYN) Conditions of TCP Header Is Limited in Use..... 1-36
Table 1-29. List of Parameters that Can Be Set for Each RP Type Using IPv6 Filter Flow Information 1-44
Table 1-30. General Protocol Number..... 1-46
Table 1-31. Relationship Between Upper and Lower IP User Data Length Limits and IP User Data Length..... 1-48
Table 1-32. General Port Number 1-48

Downloaded from www.Manualslib.com manuals search engine

Table 1-33. General ICMPv6 Type and Code Number 1-49
Table 1-34. List of Interfaces that Support Flow Control 1-50
Table 1-35. Maximum Definable Entries by Model and Each PM Mounting Memory Size 1-58
Table 1-36. List of Parameters that Can Be Set for Each RP Type Using IPv4 QoS Information 1-61
Table 1-37. Operating Parameters that Can Be Set for Each Operation 1-64
Table 1-38. General protocol number 1-66
Table 1-39. Relationship Between Upper and Lower IP User Data Length Limits and IP User Data Length 1-67
Table 1-40. General ICMP Type Code Number 1-68
Table 1-41. Genral IGMP Type Code Number 1-69
Table 1-42. General ICMP type number 1-69
Table 1-43. Relationship Between Number of Queues and Priority 1-72
Table 1-44. Relationship Between Number of Queues and Priority 1-74
Table 1-45. Number of Entries Used per List by Each Setting 1-75
Table 1-46. List of Parameters that Can Be Set for Each RP Type Using IPv6 QoS Information. 1-85
Table 1-47. Operating Parameters that Can Be Set for Each Operation 1-87
Table 1-48. General Protocol Number 1-89
Table 1-49. Relationship Between Upper and Lower IP User Data Length Limits and IP User Data Length 1-91
Table 1-50. General ICMP Type Code Number 1-92
Table 1-51. General IGMPv6 Type Code Number 1-92
Table 1-52. Relationship Between Number of Queues and Priority Setting Condition Range 1-95
Table 1-53. Relationship between number of queues and priority 1-97
Table 1-54. Number of Entries Used per List by Each Setting 1-98
Table 1-55. Features of Constituting Definition of Filter Flow Information by Input Form 1-107
Table 1-56. Applicable Parameters by Upper Protocol 1-111
Table 1-57. Filtering Condition Derived from Relation between Limit Setting Parameter and IP User Data Length 1-112
Table 1-58. Corresponding Values - *tos <Value>* *1-112*
Table 1-59. Corresponding Values - *Diff-serv* *1-113*
Table 1-60. Combination of Pair Switch 1-117
Table 1-61. Combined Setting of Pair Switch and Possibility of Use 1-117
Table 1-62. Packet Type in which the Filtering Based on the Flag (ACK and SYN) Conditions of TCP Header Is Limited in Use 1-118
Table 1-63. IGMP Type Number 1-119
Table 1-64. Replace_TOS Field Rewriting 1-120
Table 1-65. Features of Constituting Definition of Filter Flow Information by Input Form 1-132
Table 1-66. Relationship Between QoS Command Effectiveness and Ineffectiveness 1-137
Table 1-67. Parameters To Be Set Per Queue Mode 1-139
Table 1-68. Maximum Range of Send Bandwidth 1-140
Table 1-69. Media Type and Available Queue Mode 1-141
Table 1-70. Categories of the Control Packets Outputted by Queue 8 or 16 1-143
Table 1-71. Parameters list in bandwidth control (traffic) 1-146
Table 1-72. Calculation Example of Excess Bandwidth 1-147
Table 1-73. List of the Parameters When GR2000-1B and GR2000-2B Band Designation (Traffic Designation) is Made. 1-147
Table 1-74. Relationship Between Priority Determination Among Minimum Bandwidth Guarantee (kbit/s), Band Control (Traffic Designation), and Flow Control 1-153
Table 1-75. Parameters That Can be Set by Each Transmission Control 1-154
Table 1-76. Interface Names 1-155
Table 1-77. Relationship Between the Physical Line That Sets the Group Band Control in the Same NIF and the Group Number That Can Be Set 1-155
Table 1-78. Range in Which a Line's Maximum Transmission Range Can Be Set 1-156
Table 1-79. List of Parameters When the Band Control (Traffic Designation) in the VLAN Line or the Group Band Control is Designated 1-156
Table 1-80. Relationship in the priority determination between the group band control and

Downloaded from www.Manualslib.com manuals search engine

the flow control 1-165
Table 1-81. Discard Mode 1-166
Table 1-82. Configurable Parameters for Flow Detection by Upper-level Protocol 1-169
Table 1-83. Configurable Flow Control Parameters by Flow-control Type 1-170
Table 1-84. Relationship Between IP User Data Length Upper/Lower Limits and IP User Total Data Length 1-171
Table 1-85. List of IGMP Type Number 1-174
Table 1-86. UPC Penalty Operation 1-176
Table 1-87. UPC Combined Setting Sequence 1-177
Table 1-88. Range of Priority Class and Discard Class 1-179
Table 1-89. Range of Priority Class and Discard Class 1-181
Table 1-90. Combination of Pair Switch 1-182
Table 1-91. Combined Setting of Pair Switch and Possibility of Use 1-183
Table 1-92. TOS Number Calculation 1-183
Table 1-93. TOS Replacing Value for Setting Value 1-184
Table 1-94. Mapping of Class No. and Queue No. (Max Output Priority is 8) 1-184
Table 1-95. Mapping of Class No. and Queue No. (Max Output Priority is 8) 1-185
Table 1-96. Mapping of Class No. and Queue No. (Max Output Priority is 32) 1-186
Table 1-97. Packet Type 1-193
Table 1-98. Initial Value Corresponding To TOS Value 1-198
Table 1-99. Mapping of TOS Value and Output/Queuing Priority Class 1-199
Table 1-100. Parameters for each queuing mode 1-214
Table 1-101. Default length of each queue 1-215
Table 1-102. Allowable Characters 1-219

Chapter 2 - IPX/Bridge Information 2-1

Table 2-1. Server Type Reference Values 2-15

Chapter 3 - SNMP Information 3-1

Table 3-1. Application of SNMP Information Objects 3-1
Table 3-2. Trap System Message Levels 3-3

Chapter 4 - Operation Management Information 4-1

Table 4-1. Location of appended manufacturing number seals 4-16
Table 4-2. List of Initial Value Items that Can Be Set Using SNMP Information and Initial Values during Initial Installation 4-34
Table 4-3. List of Initial Value Items that Can Be Set Using line Information (Ethernet /Gigabit Ethernet) and Initial Values During Initial Installation 4-35
Table 4-4. List of Initial Value Items that Can Be Set Using line Information (WAN) and Initial Values During Initial Installation 4-37
Table 4-5. List of Initial Value Items that Can Be Set Using line Information (WAN OC-POS) and Initial Values during Initial Installation 4-39
Table 4-6. List of Initial Values That Can Be Set Using Line Information (ATM Information) and Initial Values During Initial Installation 4-40
Table 4-7. List of Initial Values That Can Be Set Using Subline Information (WAN Line) and Initial Values During Initial Installation 4-41
Table 4-8. List of Initial Values that Can Be Set Using PPP Information and Initial Values During Initial Installation 4-42
Table 4-9. List of Initial Values That Can Be Set Using PPPoE Information and Initial Values During Initial Installation 4-43
Table 4-10. List of Initial Values that can be set using Frame Relay Information and Initial Values during Initial Installation 4-45

Downloaded from www.Manualslib.com manuals search engine

Table 4-11. List of Initial Values That Can Be Set Using ARM Information and Initial Values During Initial Installation 4-47
Table 4-12. List of Initial Values That Can Be Set Using ISDN Information and Initial Values During Initial Installation 4-49
Table 4-13. List of Initial Values That Can Be Set Using Tunnel Information and Initial Values During Initial Installation 4-51
Table 4-14. List of Default Values That Can Be Set Using IP Information and Default Values During Initial Installation 4-52
Table 4-15. List of Default Values That Can Be Set Using NAT-PT Information and Default Values During Initial Installation 4-53
Table 4-16. List of Initial Values That Can Be Set Using IPX Information and Initial Values During Initial Installation 4-55
Table 4-17. List of Initial Values That Can Be Set Using IPX Information and Initial Values During Initial Installation 4-56
Table 4-18. List of Initial Values That Can Be Set Using QoS Information and Initial Values During Initial Installation 4-58
Table 4-19. List of Initial Values That Can Be Set Using Filter Information and Initial Values During Initial Installation 4-59

Chapter 5 - Configuration Error Messages 5-1

Table 5-1. Configuration Error Messages 5-2
Table 5-2. Router Control Information Error Messages 5-3
Table 5-3. Network Interface Error Messages 5-4
Table 5-4. IP Information Error Messages 5-14
Table 5-5. Routing Protocol Error Messages 5-20
Table 5-6. Multicast Router Control Information Error Messages 5-52
Table 5-7. IPv6 Multicast Router Control Information Error Messages 5-62
Table 5-8. Flow Information Error Messages 5-64
Table 5-9. Filter and QoS Information (Other than Flow Information) Error Messages 5-76
Table 5-10. MPLS Information Error Messages [ROUTE-OS7] 5-83
Table 5-11. IPX Information Error Messages 5-88
Table 5-12. Bridge Information Error Messages 5-91
Table 5-13. VRRP Information Error Messages 5-92
Table 5-14. SNMP Information Error Messages 5-93
Table 5-15. COPS Information Error Messages 5-94
Table 5-16. RADIUS Error Messages 5-95
Table 5-17. Operation Management Information Error Messages 5-96
Table 5-18. Address Translaion Information Error Messages 5-97
Table 5-19. DHCP Server Information Error Messages 5-99
Table 5-20. DHCP Client Information Error Messages 5-100
Table 5-21. NAT-PT Error Messages 5-100
Table 5-22. DNS Resolver Information Error Messages 5-101
Table 5-23. Log Information Error Messages 5-101
Table 5-24. E-Mail Sending Information Error Messages 5-101
Table 5-25. Other Error Messages 5-102

Index Index-1

Downloaded from www.Manualslib.com manuals search engine

Chapter 1
Filtering/QoS Information

This is the second of two volumes detailing the configuration commands for the Hitachi GR2000 Gigabit Router Series. This manual is organized into five chapters:

- Chapter 1 provides information regarding filtering and QoS, including flow information, QoS objects, and COPS.
- Chapter 2 covers IPX and bridge objects
- Chapter 3 covers SNMP objects
- Chapter 4 provides operation management information, including information about host name, logs, NTP, board disablement, and default configuration objects.
- Chapter 5 is a complete list of all configuration error messages.

The first volume of commands, *Hitachi Gigabit Router GR2000 Series Enhanced Version Configuration Commands, Vol. 1*, covers the following areas in seven chapters:

- Chapter 1 provides a configuration command overview, and an introduction to configuration subcommands.
- Chapter 2 describes the router management object - *router*.
- Chapter 3 provides command information about the network interface, including line objects, link layer protocol objects, ISDN objects, the group information object - group, tunnel information, and backup.
- Chapter 4 cover IP commands, including IP information objects, ndp, ra, VRRP, policy routing, DHCP relay, DHCP server, and DHCP client information, and address translation information.
- Chapter 5 provides information about IP routing protocol objects
- Chapter 6 is for IP and IPv6 multicast routing protocol commands.
- Chapter 7 covers MPLS commands.

In addition, the *Hitachi Gigabit Router GR2000 Series Enhanced Version Configuration Settings* manual provides extensive configuration examples contained in the following three chapters:

- Chapter 1 is general information about configuration
- Chapter 2 is a configuration overview
- Chapter 3 provides configuration examples for the commands covered in both volumes of configuration command manuals.

Downloaded from www.Manualslib.com manuals search engine

1.1 Flow Information

The flow control can be divided into the IPv4 flow control noticing on the IPv4 packet and the IPv6 noticing on the IPv6 packet. Explanations are given hereunder on the respective functions, followed by explanations on the constituting definition commands and parameters that define the information given about this flow control.

1.1.1 IPv4 Flow Control

The IPv4 flow control is provided with the filter function to relay or discard the packet and the QoS function (the flow control part) to decide the priority for signaling by packet types.

The flow control is set on both interface's input and output side.. The first stage executes mainly the filter function while the second stage executes mainly the QoS function (flow control part) in each of the input and output sides. The packet performs determination on the flow control in the order of (a) the filter function on the first input side stage, (b) the QoS function on the second input side stage, (c) the filter function on the first output side stage, and (d) the QoS function on the second output side stage.

A brief explanation on the contents is given on each control block constituting the flow control as are the related constituting definition commands.

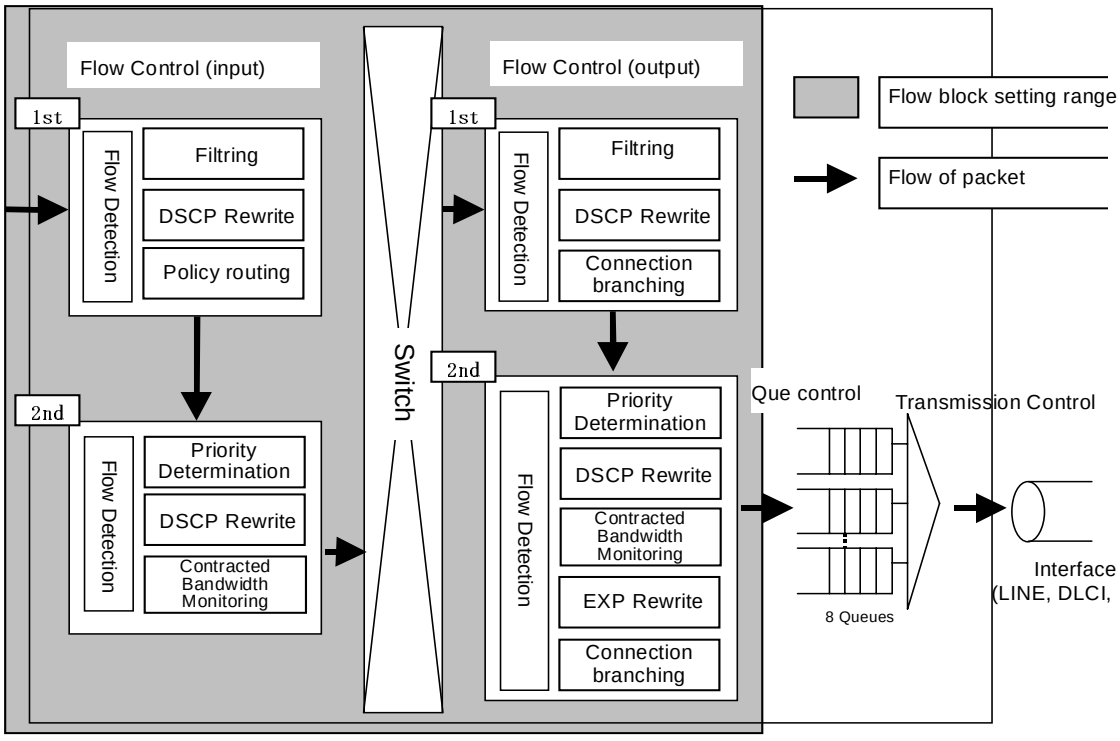


Figure 1-1 Range of QoS, Filter-Flow Control

Downloaded from www.Manualslib.com manuals search engine

- Filter function on the first input side stage

  The first input side stage executes the following functions:

  Filtering: Relays or discards the packet in accordance with the flow detecting condition.

  DSCP rewriting: Rewrites the DSCP field in accordance with the flow detecting condition.

  Policy routing: Transmits the packet to the specified output destination in accordance with the flow detecting condition.

  Constituting definition command → 1, 2 flow filters (filter flow information)

- QoS function on the second input side stage (flow control part)

  The second input side stage executes the following functions:

  Priority determination:
  Determines the priority of the packet that agrees with the flow detecting condition.

  DSCP rewriting: Rewrites the DSCP field of the packet that agrees with the flow detecting condition.

  Contract band monitoring:
  Monitors if the packet that agrees with the flow detecting condition is following or violating the contract band.

  Constituting definition command → 1, 3 flow filters (QoS flow information)

- Filter function on the first output side stage

  The first input side stage executes the following functions:

  Filtering: Relays or discards the packet in accordance with the flow detecting condition.

  DSCP rewriting: Rewrites the DSCP field in accordance with the flow detecting condition.

  Connection branching:
  Selects and transmits the packet to the specified DLCI/VC in accordance with the flow detecting condition.

  Constituting definition command → 1, 2 flow filters (filter flow information)

- Filter function on the second output side stage (flow control part)

  The second output side stage executes the following functions:

  Priority determination:
  Determines the priority of the packet that agrees with the flow detecting condition.

  DSCP rewriting: Rewrites the DSCP field of the packet that agrees with the flow detecting condition.

  Contract band monitoring:
  Monitors if the packet that agrees with the flow detecting condition is following or violating the contract band.

  EXP rewriting: Rewrites the EXP field of the packet that agrees with the flow detecting condition.

Downloaded from www.Manualslib.com manuals search engine

Connection branching:

Selects and transmits the packet to the specified DLCI/VC in accordance with the flow detecting condition.

Constituting definition command → 1, 3 flow filters (QoS flow information)

- Interlocking with QoS transmission control

  Queue mode shall be set to control the sequence of outputting a packet to the transmission queue in the interface. The queue mode includes the following five catergories: output priority control, minimum band assurance, uniformity assurance, minimum uniformity band assurance, and minimum band assurance (kbps designation). The definition method defines a queue list to be set in the transmission queue of the interface by using the QoS attribute (qos-queue-list) and further sets a queue list to be used on each interface by using the QoS interface information (qos-interface).

  → 3.2 qos-queue-list (Qos queue attribute)

  → 3.3 qos-interface (QoS interface information)

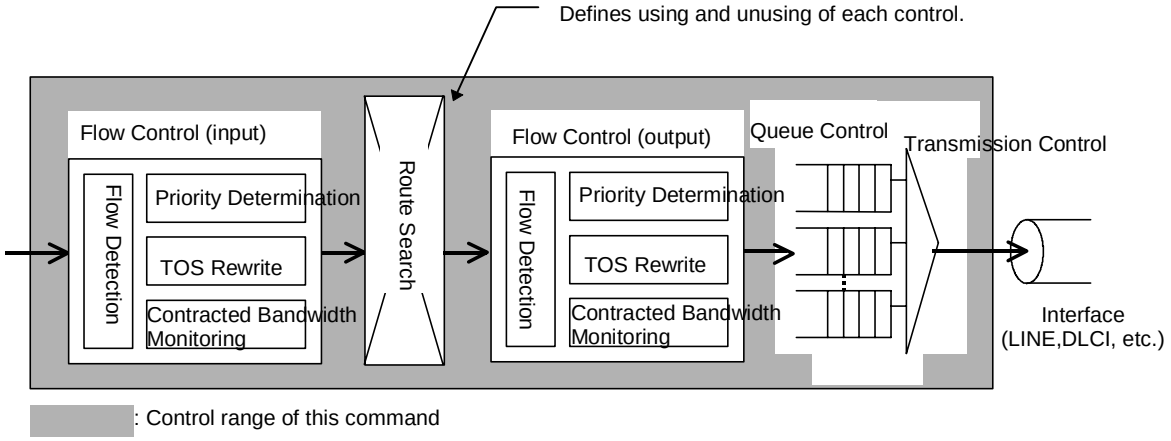


Figure 1-2 Control Range for QoS Queue Attribute and QoS Interface Information

- Interlocking with QoS queue control

  The queue control is a function that discards a packet to be stacked on the transmission queue according to the queuing priority if the packet is stagnating in the transmission queue. The function sets the pattern of queue length permitting the queuing on each queuing priority by using the QoS discard mode (qos-discard-mode).

Downloaded from www.Manualslib.com manuals search engine

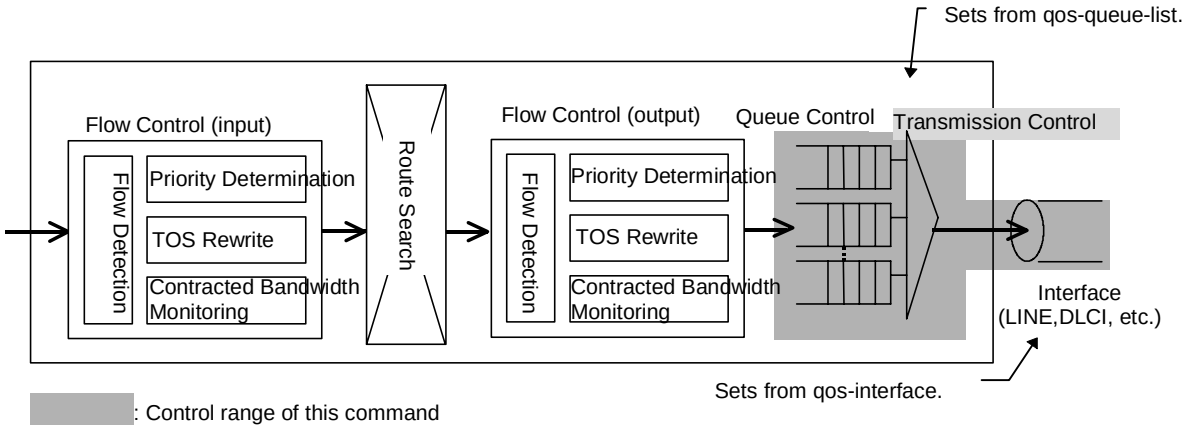


Figure 1-3 Control Range for QoS Discard Mode

Precautions

The inputting form for the filter flow information includes the following two forms: the flow filter constituting definition information, and the filter-list, filter-group and filter-interface constituting definition information. The features of each inputting form are shown in Table 1-1.

Table 1-1 Features of Each Constituting Definition Inputting Form for Filter Flow Information

Item	Constituting Definition Iinput Form	
	filter-list, filter-group, filter-interface	***flow filter***
Number of entry(*1)	1024 entry/device	10000 entry/device 2000 entry/RP
Inputting form	Input three commands to define one list. Effective in defining the same flow control in multiple number of input/output interfaces.	Input one command to define one list. Effective in inputting a number of entries.
Function use, and unused unit	Device unit	Device unit, and input/output interface unit
GR2000 Operations Commands, Vol. 2 - Indication unit for fshow filter-flow	Device unit and list unit	Input/output interface unit, and list unit
RM Ethernet	Supported.	Unsupported.
VLAN ID detection	Unsupported	Supported
Display of entry count used	Unsupported	Supported
Filtering of local packet that coincides with the flow detection conditions of configuration definition information	During default setting, the local packet that coincides with the flow detection conditions of configuration definition information is not treated for filtering. Whether to treat the local packet for filtering is determined using a parameter.	During default setting, the local packet that coincides with the flow detection conditions of configuration definition information is treated for filtering. No parameter is provided.
**1: For more details, refer to Table 1-20, "Maximum Definable Entries by Each PM Mounting Memory Size," on page 1-25.*		

Downloaded from www.Manualslib.com manuals search engine

Precautions

The inputting form for the QoS flow information includes the following two forms: the flow QoS constituting definition information, and the qos-ip-list, qos-ip-list-group and qos-ip constituting definition information. The features of each inputting form are shown in Table 1-2.

Table 1-2 Feature of Constituting Definition of QoS Flow Information by Each Input Form

Item	Constituting Definition Input Form	
	qos-ip-list, qos-ip-list-group, qos-ip	**flow filter**
Number of entry (*1)	1024 entry/device	10000 entry/device 2000 entry/RP
Inputting form	Input three commands to define one list. Effective in defining the same flow control in multiple number of input/ output interfaces.	Input one command to define one list. Effective in inputting a number of entries.
Function use, and unused unit	Device unit	Device unit, and input/output interface unit
GR2000 Operations Commands, Vol. 2 - Indication unit forshow qos ip-flow.	Device unit and list unit	Input/Output interface unit, and list unit
Determination of arbitrary priority in all IP packets (*2)	Unsupported	Supported (Except RP-A1)
Display of entry count used	Unsupported	Supported

**1: For more details, refer to Table 1-35, "Maximum Definable Entries by Model and Each PM Mounting Memory Size," on page 1-58.*
**2: There is a packet of which priority is fixedly determined irrespective of the setting contents of configuration definition information.*

1.1.2 IPv6 Flow Control

The IPv6 flow control has a filter function and QoS function. The input format of IPv6 flow information is the flow configuration definition information described in this chapter.

For the configuration definition command of IPv6 filter flow information, refer to 1.1.4, "flow filter (Filter Flow Information)," on page 1-24."

For the configuration definition command of IPv6 QoS flow information, refer to 1.1.7, "flow qos (QoS Flow Information)," on page 1-57."

Caution: The features of a flow filter input format are shown in Table 1-3 Features for Each Configuration Definition Input Format of Filter Flow Information.

Downloaded from www.Manualslib.com manuals search engine

The features of a flow filter input format are listed in Table 1-4.

Table 1-3 Features of Each Constituting Definition Inputting Form for *flow filter* Information

Item	Configuration Input Format
	flow filter
Number of entry (*1)	Refer to Table 1-20, “Maximum Definable Entries by Each PM Mounting Memory Size,” on page 1-25.
Inputting form	Input one command to define one list. Effective in inputting a number of entries.
Function use, and unused unit	Device unit Device unit, and input/output interface unit
Operation command Indication unit for filter ip flow.	Input/output interface unit, and list unit
RM Ethernet Supported.	Unsupported.
**1: There is a packet of which priority is fixedly determined irrespective of the setting contents of configuration definition information.*	

The features of a flow qos input format are listed in Table 1-4.

Table 1-4 Features of Each Constituting Definition Inputting Form for *flow qos* Information

Item	Configuration Input Format
	flow qos
Number of entry (*1)	Refer to Table 1-20, “Maximum Definable Entries by Each PM Mounting Memory Size,” on page 1-25.
Inputting form	Input one command to define one list. Effective in inputting a number of entries.
Function use, and unused unit	Device unit Device unit, and input/output interface unit
Operation command Indication unit for filter ip flow.	Input/output interface unit, and list unit
Determination of arbitrary priority in all IP packets (*1)	Supported.
**1: There is a packet of which priority is fixedly determined irrespective of the setting contents of configuration definition information.*	

Interface Types that Support Flow Control

Table 1-5 is a list of interfaces that support flow control. The listed interfaces support IPv4 and IPv6 flow controls. These interfaces designate applicable interface names set by the ip information or the ip-address information. (The IP information or the IP-address information must be set before setting the flow control.)

Downloaded from www.Manualslib.com manuals search engine

Table 1-5 List of Interfaces that Support Flow Control

Interface Name	IPv4				IPv6			
	flow filter		*flow qos*		*flow filter*		*flow qos*	
	Input Side	Output Side	Input Side	Output Side	Input Side	Output Side	Input Side	Output Side
<Line Name>	√	√	√	√	√	√	√	√
rmEthernet	---	---	---	---	---	---	---	---
<DLCI Name>	√	√	√	√	√	√	√	√
<VC Name>	√	√	√	√	√	√	√	√
<Group Name>	√	√	√	√	√	√	√	√
<Timeslot Name>	√	√	√	√	√	√	√	√
<Peer Name>	√	√	√	√	√	√	√	√
<Tunnel Name>	√	√	---	---	√	√	---	---
<VLAN Name>	√	√	√	√	√	√	√	√
<Session Name>	--- (1*)	√ (2*)	---(1*)	√ (2*)	--- (1*)	√ (2*)	---(1*)	√ (2*)

÷: Setting possible.
-: Setting impossible
**1: PPPoE session (input side) are not supported.*
**2: Only 1 session is supported.*

Cautions during BCU replacement

RP is rebooted when BCU replacement is executed in devices in which the flow configuration information of the current configuration definition information has been changed. In order to limit RP reboots during the BCU replacement, execute the procedure below for the active system BCU.

1. Config save configuration definition command entry
2. Config close configuration definition command entry
3. Config copy configuration definition command entry
   Example: config copy/mc0/config/router.caf primary
4. Execute BCU replacement

Types of action that have an affect when using filter flow information and QoS flow information in combination

The activation priority when using filter flow information and QoS flow information in combination in the same interface is as indicated below (*1).

Input filter < input QoS < output filter < output QoS

Therefore, when using in combination with DSCP rewrite or connection branch when filter flow information or QoS flow information activation is specified, the setting with the highest activation priority is enabled. When setting policy with filter flow information and setting EXP rewrite with QoS flow information, activation is executed by the activation designation defined by QoS flow information.

Downloaded from www.Manualslib.com manuals search engine

Table 1-6 Types of action that have an affect when using filter flow information and QoS flow information in combination

Types of action	Flow control	Effect
Filtering	filter flow information	--
DSCP rewrite	filter flow information, Qos flow information	X
Policy routing	filter flow information	√
Connection branch	filter flow information	X
Output priority definition	Qos flow information	--
User priority rewrite	Qos flow information	--
Contract band monitoring	Qos flow information	--
EXP rewrite	Qos flow information	--

√: Setting is disabled when EXP rewrite is defined by flow qos (QoS flow information)
X: The setting with the highest activation priority is enabled.
-: No effect
**1 Conditioned on coincidence in the flow of the flow setting conditions of each definition.*

1.1.3 *flow* (Flow Information)

The flow control function is set. This command cannot be set when setting the constituting definition qos-ip-list or the constituting definition filter-list. Further, when setting this command, the constituting definition qos-ip-list or the constituting definition filter-list cannot be set.

Input Form

Setting the information

```
[set] flow [{-no | -yes}] [{-classify_all_off | -classify_all}]
[-cops_range <Minimum List No.>-<Maximum List No.>]
[{-l2upc_off | -l2upc}]
[{-precedence_mask_off | -precedence_mask}]
```

Changing the information

```
[set] flow [{-no | -yes}][{-classify_all_off | -classify_all}]
[-cops_range <Minimum List No.>-<Maximum List No.>]
[{-l2upc_off | -l2upc}]
[{-precedence_mask_off | -precedence_mask}]
```

Deleting the information

```
delete flow
```

Indicating the information

```
show flow
```

Displays the number of entries in the set filter list and QoS list.

```
show flow used_resources
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

[{-no | -yes}]

Description: Specifies use or no-use of the flow control function.

-no : Not used.

-yes : Used.mParameter

Default: no

[{ -classify_all_off | -classify_all }] :

This parameter fixedly specifies the priority of an IPv4 packet that this router generates or specifies it using a flow qos command. It is invalid in RP-A1. In RP-A1, this parameter operates as classify_all_off. The IPv6 packet that this router generates is controlled by the priority set using a flow qos command irrespective of the existence of this option.

-classify_all_off :

This parameter specifies the fixed priority in the IP packet that this router generates. The priority for each packet type when this parameter is specified is shown in Table 1-8 on page 1-12.

-classify_all:

This parameter specifies the priority, set using a flow qos command, in the IP packet that this router generates. The priority for each packet type when this parameter is specified is shown in Table 1-9 on page 1-13.

Default: -classify_all_off

Range of value: None

[-cops_range <Minimum List No.>-<Maximum List No.>[Ver. 06-03]

Description: This parameter specifies the range of a flow list number in which a COPS agent function can be set to all RPs. It cannot be changed when "cops_yes" is set in the cops configuration definition. Also, this parameter cannot be deleted when cops configuration definition is set.

Default: None (A COPS function is not used.)

Range of value: 1 to 20000 (decimal)

Note 1: The calculation expression for obtaining RP unit yen and numeric characters is described below.
Number RP unit entries = <Maximum List No.> - <Minimum List No.> + 1
An example of calculation for the number of entries is given below.
For -cops range 1001 - 2000
2000 - 1001 + 1 = 1000
The number of flow list entries that can be set using a COPS agent function is 1000 in units of RP.
This parameter can set a maximum of 2000 entries per RP.

Downloaded from www.Manualslib.com manuals search engine

[{ -l2upc_off | -l2upc }]

Description: Contract bandwidth monitoring is executed based on the length of from MAC header to FCS of sent and received packets. This parameter is enabled when combined with -upc, -max rate and -min rate. When setting this parameter in RP-A1, RP-C and RP-D, contract bandwidth monitoring is executed based on length excluding the MAC header and FCS of sent and received packets. A list of supported L2 UPC functions for each RP type is indicated in Table 1-7, Supported L2 UPC functions for each RP type.

-l2upc_off:
Bandwidth monitoring is executed based on length excluding the MAC header and FCS of sent and received packets.

-l2upc:
Bandwidth monitoring is executed based on length from the MAC header to FCS of sent and received packets.

Default: -l2upc_off

Range of value: None

Table 1-7 Supported L2 UPC functions for each RP type

Item			Supported L2 UPC functions for each RP type
RP type		RP-A1,RP-C,RP-D	RP-C6,RP-D6, RP-CV,RP-DV, GR2000-1B,GR2000-2B,GR2000-2B+,GR2000-BH
L2 UPC function support		--	√
Supported interface		--	LAN interface
L2 header setting value (*1)	no VLAN identifier	--	18 bytes
	VLAN identifier	--	22 bytes
	Other than above	--	0 byte

√: Setting possible
-: Setting not possible
**1: Only Ethernet V2 format frames are supported. Therefore, errors occur with bandwidth monitoring in 802.3 format frames. In addition, errors also occur with bandwidth monitoring in PPP frames and MPLS frames in Ethernet.*

[{-precedence_mask_off | -precedence_mask}]

Description: Enables the upper 3 bits of the ToS field of sent and received packets as flow detection conditions. When this parameter is set, only the upper 3 bits (precedence value) of the specified DSCP value are enabled even if the DSCP value of flow detection conditions is set for the device overall.

-precedence_mask_off:
Enables the DSCP value of sent and received packets as flow detection conditions.

-precedence_mask:
Enables the precedence value of sent and received packets as flow detection conditions.

Default: -precedence_mask_off

Range of value: None

Downloaded from www.Manualslib.com manuals search engine

used_resources

Description: Displays the number of entries in the set filter list and QoS list.

Default: Cannot be omitted when the number of entries is displayed.

Table 1-8 Priority for Each Packet Type When *classify_all_off* is Specified (All Models Except GR2000-1B and GR2000-2B)

Packet Type	State of IP Flow Detection Conditions	Output Priority (*1) (*2)					Queuing Priority
		8 Queue	16 Queue	32 Queue	250 Queue	1000 Queue	
ARP (ARP Request/ARP Response) packet generated by this router	--	8	16	32	250	1000	4
Layer 2 packet generated by this router (WAN)	--	8	16	32	250	1000	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides/Does not coincide	8	16	32	250	1000	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides/Does not coincide	4	7	13	98	392	1
IPv4 packets relayed by this router: 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides/Does not coincide	4	7	13	98	392	4
MPLS packets (MPLS LDP Hello, MPLS LDP KeepAlive, etc.) generated by this router **[ROUTE-OS7]**	Coincides/Does not coincide	8	16	32	250	1000	4
IPv4 packets except in item Nos. 3 to 6	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	4
IPv6 packet generated by this router (Except in item No. 9) (*3)	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	8	16	32	250	1000	4
IPv6, ICMP to notice a error generated by this router (*3)	Coincides.	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	1
IPv6 packet relayed by this router (*3)	Coincides.	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: This function can specify the priority of all IP packets by flow configuration definition.*
**2: The output priority indicates the queue number for stacking packets.*
**3: GR2000-2S and GR2000-4S in which RP-A1, RP-C, and RP-D are installed has the same priority level as when it mismatches the flow detection conditions because IPv6 QOS is not supported.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-9 Priority for Each Packet Type When *classify_all* is Specified (All Models Except GR2000-1B, GR2000-2B and GR2000-2B+)

Packet Type	State of IP Flow Detection Conditions	Output Priority (*1) (*2)					Queuing Priority
		8 Queue	16 Queue	32 Queue	250 Queue	1000 Queue	
ARP (ARP Request/ARP Response) packet generated by this router	--	8	16	32	250	1000	4
Layer 2 packet generated by this router (WAN)	--	8	16	32	250	1000	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	8	16	32	250	1000	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	4
IPv4 packets relayed by this router: 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	4
MPLS packets (MPLS LDP Hello, MPLS LDP KeepAlive, etc.) generated by this router [ROUTE-OS7]	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	8	16	32	250	1000	4
IPv4 packets except in item Nos. 1 to 6	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide.	4	7	13	98	392	4
IPv6 packet generated by this router (*3)	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	8	16	32	250	1000	4
IPv6, ICMP packet to notice a error generated by this router (Except in item No. 9) (*3)	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	1
IPv6 packet relayed by this router (*3)	Coincides	Priority specified by flow qos configuration definition					
	Does not coincide	4	7	13	98	392	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: This function can specify the priority of all IP packets by flow configuration definition.*
**2: The output priority indicates the queue number for stacking packets.*
**3: GR2000-2S and GR2000-4S in which RP-A1, RP-C, and RP-D are installed has the same priority level as when it mismatches the flow detection conditions because IPv6 QOS is not supported.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-10 Priority for Each Packet Type When *classify_all_off* is Specified (For all Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control)

Packet Type	State of IP Flow Detection Conditions	Output Priority (*1) (*2)							Queuing Priority
		4 Queue	8 Queue	16 Queue	32 Queue	64 Queue	250 Queue	1000 Queue	
ARP (ARP Request/ARP Response) packet generated by this router	--	4	8	16	32	64	250	1000	4
Layer 2 packet generated by this router (WAN)	--	4	8	16	32	64	250	1000	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides/ Does not coincide	4	8	16	32	64	250	1000	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides/ Does not coincide	2	4	7	13	25	98	392	1
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides/ Does not coincide	2	4	7	13	25	98	392	4
IPv4 packets except in item Nos. 3 to 5	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	4
IPv6 packet generated by this router (Except in item No. 9)	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	4	8	16	32	64	250	1000	4
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	1
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: This function can specify the priority of all IP packets by flow configuration definition.*
**2: The output priority indicates the queue number for stacking packets.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-11 Priority for Each Packet Type When *classify_all_off* is Specified (All Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control)

Packet Type	State of IP Flow Detection Conditions	Output Group Number and Output Priority (*1)		Queuing Priority
		Up to the Nnumber of Group of 2	More than the Nnumber of Group of 3	
ARP (ARP Request/ARP Response) packet generated by this router	--	(Group 1) 4	(Group 16) 4	4
Layer 2 packet generated by this router (WAN)	--	(Group 1) 4	(Group 16) 4	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides/Does not coincide	(Group 1) 4	(Group 16) 4	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides/Does not coincide	(Group 1) 2	(Group 8) 1	1
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides/Does not coincide	(Group 1) 2	(Group 8) 1	4
IPv4 packets except in item Nos. 3 to 5	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	4
IPv6 packet generated by this router (Except in item No. 9)	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 4	(Group 16) 4	4
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	1
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: This function can specify the priority of all IP packets by flow configuration definition. The number of queued entries in the output group is fixed at four.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-12 Priority for Each Packet Type When *classify_all* is Specified (All Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control)

Packet Type	State of IP Flow Detection Conditions	Output Priority (*1) (*2)							Queuing Priority
		4 Queue	8 Queue	16 Queue	32 Queue	64 Queue	250 Queue	1000 Queue	
ARP (ARP Request/ARP Response) packet generated by this router	--	4	8	16	32	64	250	1000	4
Layer 2 packet generated by this router (WAN)	--	4	8	16	32	64	250	1000	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	4	8	16	32	64	250	1000	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	1
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	4
IPv4 packets except in item Nos. 1 to 5	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	4
IPv6 packet generated by this router (Except in item No. 9)	Coincides	Priority specified by flow qos configuration definition							
	Does not coincide	4	8	16	32	64	250	1000	4
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	1
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition							
	Does not coincide	2	4	7	13	25	98	392	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: This function can specify the priority of all IP packets by flow configuration definition.*
**2: The output priority indicates the queue number for stacking packets.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-13 Priority for Each Packet Type When *classify_all* is Specified (All Models Except GR2000-1B, GR2000-2B, GR2000-2B+ and Group Band Control)

Packet Type	State of IP Flow Detection Conditions	Output Group Number and Output Priority (*1)		Queuing Priority
		Up to the Nnumber of Group of 2	More than the Nnumber of Group of 3	
ARP (ARP Request/ARP Response) packet generated by this router	--	(Group 1) 4	(Group 16) 4	4
Layer 2 packet generated by this router (WAN)	--	(Group 1) 4	(Group 16) 4	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 4	(Group 16) 4	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	1
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	4
IPv4 packets except in item Nos. 3 to 5	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	4
IPv6 packet generated by this router (Except in item No. 9)	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 4	(Group 16) 4	4
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	1
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	(Group 1) 2	(Group 8) 1	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: This function can specify the priority of all IP packets by flow configuration definition. The number of queued entries in the output group is fixed at four.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-14 Priority for Each Packet Type When -classify_all_off is Specified (GR2000-BH)

Packet Type	State of IP Flow Detection Conditions	Output Priority (*1) (*2)		Queuing Priority
		8 Queue	32 Queue	
ARP (ARP Request/ARP Response) packet generated by this router	--	8	32	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides/Does not coincide	8	32	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides/Does not coincide	4	13	1
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides/Does not coincide	4	13	4
IPv4 packets except in item Nos. 2 to 4	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	4
IPv6 packet generated by this router (Except in item No. 7)	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	8	32	4
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	1
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: The output priority indicates the queue number for stacking packets.*
**2 This indicates the output priority for each output line queue number (8.32).*

Downloaded from www.Manualslib.com manuals search engine

Table 1-15 Priority for Each Packet Type When -classify_all is Specified (GR2000-BH)

Packet Type	State of IP Flow Detection Conditions	Output Priority (*1)(*2)		Queuing Priority
		8 Queue	32 Queue	
ARP (ARP Request/ARP Response) packet generated by this router	--	8	32	4
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	8	32	4
IPv4 ICMP packet for reporting the error generated by this router	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	4
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	4
IPv4 packets except in item Nos. 2 to 4	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	4
IPv6 packet generated by this router (Except in item No. 7)	Coincides	Priority specified by flow qos configuration definition		
	Does not coincide	8	32	4
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	1
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition		
	Does not coincide	4	13	4

--: Does not agree with the IP flow detecting condition because it is not the IP packet.
**1: The output priority indicates the queue number for stacking packets.*
**2 This indicates the output priority for each output line queue number (8.32).*

Downloaded from www.Manualslib.com manuals search engine

Table 1-16 Priority for Each Packet Type When -classify_all_off is Specified (NE1G-2D)

Packet Type	State of IP Flow Detection Conditions	Output line queue number	Queuing Priority
ARP (ARP Request/ARP Response) packet generated by this router	--	Others	2
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides/Does not coincide	1	2
IPv4 ICMP packet for reporting the error generated by this router	Coincides/Does not coincide	1	2
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides/Does not coincide	1	2
MPLS packet generated by this router (MPLS LDP Hello, MPLS LDP Keep Alive etc.) [ROUTE-OS7]	Coincides/Does not coincide	1	2
IPv4 packets except in item Nos. 2 to 5	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv6 packet generated by this router (Except in item No. 8)	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2

--: Does not agree with the IP flow detecting condition because it is not the IP
Others: Accumulates packets in queues not subject to shaping.
*(*1): Correspondence between user priority and the send queue number is indicated in Table 1-18, Relationship between user priority and send queue number.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-17 Priority for Each Packet Type When -classify_all is Specified (NE1G-2D)

Packet Type	State of IP Flow Detection Conditions	Output line queue number	Queuing Priority
ARP (ARP Request/ARP Response) packet generated by this router	--	Others	2
IPv4 packets generated by this router (RIP, OSPF, BGP, telnet, ftp, snmp, igmp, pim, etc.)	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv4 ICMP packet for reporting the error generated by this router	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv4 packets relayed by this router 1. Packet with option (IP header) 2. Fragmented packet 3. Redirected packet 4. ARP unsolved packet 5. DVMRP-capsulated packet sent to the DVMRP tunnel interface	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
MPLS packets generated by this router (MPLS LDP Hello, MPLS LDP Keep Alive, etc.) [ROUTE-OS7]	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv4 packets except in item Nos. 1 to 6	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv6 packet generated by this router (Except in item No. 9)	Coincides	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv6, ICMP to notice a error generated by this router	Coincides.	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2
IPv6 packet relayed by this router	Coincides.	Priority specified by flow qos configuration definition (*1)	
	Does not coincide	1	2

--: Does not agree with the IP flow detecting condition because it is not the IP
Others: Accumulates packets in queues not subject to shaping.
*(*1): Correspondence between user priority and the send queue number is indicated in Table 1-18, Relationship between user priority and send queue number.*

Table 1-18 Relationship between user priority and send queue number

Priority	Discard threshold	User priority	Send queue number
Low ↕ High	Low	0	1
	High	1	
	Low	2	2
	High	3	
	Low	4	3
	High	5	
	Low	6	4
	High	7	

Downloaded from www.Manualslib.com manuals search engine

Input Examples

1. Setting the parameter:

   The flow control function is set to the use mode.

```
(config)# flow -yes
(config)#  show flow
flow yes;
(config)#
```

2. Deleting the parameter:

   The contents set for the flow control function are deleted.

```
(config)#  show flow
flow yes;
(config)#  delete flow
(config)#
```

3. Determine the priority of all IP packets freely.

   Specify the packet, whose source IP address is 10.10.10.1, destination IP address is 10.10.10.5, upper protocol is UDP, and destination port number is 161 (snmp), as output priority 1.

```
(config)# flow -classify_all
(config)#  show flow
flow yes {
         classify_all;
         qos Tokyo1 out {
                list 1 udp 10.10.10.1 10.10.10.5 161 action priority 1;
         };
};
(config)#
```

4. Designation of flow list number in which COPS agent function can be set. Flow list numbers 1 to 500 are designated as the flow list in which a COPS agent function can be set.

```
(config)# flow -cops_range 1-500
(config)#  show flow
flow yes {
         cops_range 1-500;
};
(config)#
```

5. Setting L2 UPC functions

   The total byte count of received TCP packets, including layer-2 header, is subject to bandwidth monitoring and packets are discarded if they exceed 6 Mbit/s.

```
(config)# flow -l2upc
(config)# show flow
flow yes {
         l2upc;
         qos Tokyo1 in {
                list 1 tcp any any action upc 6000;
         };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Indicating the set information:

   All the contents set for the flow control function are indicated.

```
(config)#  show flow
flow yes {
        filter Tokyo1 in {
                list 1 ip 10.10.11.5 any action forward;
                list 2 tcp 10.10.10.1 23 any action replace_iscp 8;
                list 3 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/56 any action forward;
                list 40010 ip any any action drop;
        };
        qos Tokyo2 out {
                list 1 ip any 20.20.20.1 action priority 5;
                list 2 tcp any 20.20.20.2 23 action priority 3 discard 1;
               list 3 icmp any 20.20.30.0/24 action priority 1 discard 1;
        };
        qos Tokyo3 out disable {
                list 10 icmp any 30.30.30.0/24 action priority 3;
        };
};
(config)#
```

7. Indicating the set filter list and Qos list entry number.

```
(config)#  show flow used_resources
RP No.  filter      qos      cops     total (free )
rp0          8       30       500       538 ( 1462)
rp1         15      111       500       626 ( 1374)
rp2        101     1000       500      1601 (  399)
rp3          0      500       500      1000 ( 1000)
rp4          0     1500       500      2000 (    0)
total      124     3141      2500      5765 ( 4235)
(config)#
```

Related Commands

flow, flow filter, flow qos, filter, filter-list, qos, qos-ip-list

Related Information

For the COPS function, see the *GR2000 Applications Guide*.

Precautions

1. This command cannot be set when setting the filter-filter (filter list information) or qos-ip-list (QoS IP frame condition information). Delete all the filter-list and qos-ip-list before setting this command.
2. In the case where log-in has been performed via the network, if the parameter of this command is changed from no to yes by using the operating constituting definition, be careful because it is possible that the filtering function may become activated. Depending on the contents of the definition of the filtering, the connection may be disrupted.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

4. -cops_range cannot be set when flow filter and flow qos list numbers that have been already used exist in the range of the specified list number.
5. A -cops_range parameter in which the number of RP unit entries exceeds 2000 cannot be set.
6. The -cops_range parameter of this command cannot be deleted when COPS configuration definition is set.
7. The setting of a cops_range parameter cannot be changed and deleted when a COPS function operates and when the information set from the policy server exists in this router. Delete the information set in this router from the policy server and then change or delete the -cops_range parameter.
8. If a condition persists in which the interface that set the flow filter and flow qos on the outbound side does not restore after overloading, the following message is displayed and RP or NIF may restart. Design the system using the relaying performance value shown in the table as reference.

   81010531 7030: yyyyyyyyyyyy RP hardware failure has been detected.

   40000901 xx40: 0001000000yy NIF has been restarted because of NIF hardware failure. (xx is an indication of seven segments, and vv is an optional value.)

Table 1-19 Relay Performance When Setting the *flow filter* and *flow qos* Commands. (Semi-Duplication Communication)

Per RP	RP Type	NIF Type	Number of Setting Entries			
			512 or Less	512	1024	2000
Band use rate (%) (*1)	RP-C, RP-C6	POS (OC-48, OC12 x 4 lines)	100%	75%	35%	15%
		POS (OC-3 x 8 lines)	100%	100%	80%	40%
		ATM (600 x 2 lines, 2155 x 4 lines)	100%	100%	90%	45%
		Gigabit Etherne (4 lines)	80%	45%	20%	8%
		Gigabit Etherne (3 lines)	100%	60%	30%	15%
		Gigabit Etherne (2 lines)	100%	100%	45%	20%
		Gigabit Etherne (1 lines)	100%	100%	100%	50%
	RP-D	Gigabit Ehternet	100%	100%	75%	35%
	RP-A1		100%	100%	40%	--(*2)

**1: Values in the table show the use rate of lines accommodated in one RP compared to the total band. There should be no problems in other combinations.*
**2: RP-A1 can be set to a maximum of 1024 entries. If the communication is not restored after restarting the device, introduce the "close rp" command/"free rp" command in order to re-actuate the applicable RP. Refer to the* GR2000 Operations Commands, Vol. 1, close up *and* free up *commands, respectively.*

9. For the IPv6 packet produced by this device, control is given in accordance with the priority set in the flow qos command regardless of the presence of "-classify all" parameter.
10. Flow information consumes 101 entries in each RP when address conversion (nat) is set. Therefore, when address conversion (nat) is set, the maximum entry count is decreased by 101 per RP capable of flow information definition.

1.1.4 *flow filter* (Filter Flow Information)

The filter flow information (filter condition to relay or discard a packet) is set. This command allows the preparation of a filter list concerning the IPv4 and IPv6 packets. Respective filter lists are decided by the list number described later.

Downloaded from www.Manualslib.com manuals search engine

The flow control is judged in the order of list numbers specified in the input/output interface of filter flow information (in the order of the display during execution of a show flow filter). Configuration definition qos-ip-list and filter-list cannot be set when this command is set.

The number of entries, in a filter list and QoS list, which can be generated is 10000 (maximum) per router and 2000 (maximum) per RP. However, the maximum number of entries that can be defined by RM-installed memory size differs. Table 1-20, below, lists the maximum number of entries that can be defined for each model and RM-installed memory size.

Table 1-20 Maximum Definable Entries by Each PM Mounting Memory Size

Model	RM Mounting Memory Size	Number of entry (*1)			
		Unit	RP unit		Tunnel
			RP Type	(Entry)	(Entry) [ROUTE-OS6]
GR2000-2S	All	1024	RP-A1	1024(*2)	--(*3)
GR2000-4S	64MB, 128MB, 192MB	1024	RP-A1, RP-C, RP-D	1024 (*2)	--(*3)
			RP-C6, RP-CV, RP-DV, RP-D6	1024	1024
	256MB or more	2000	RP-A1	1024 (*2)	--(*3)
			RP-C, RP-D	2000 (*2)	
			RP-C6, RP-CV, RP-DV, RP-D6	2000	2000
GR2000-6H	64MB, 128MB, 192MB	1024	RP-A1, RP-C, RP-D	1024 (*3)	--(*3)
			RP-C6, RP-D6, RP-CV, RP-DV	1024	1024
	256MB or more	6000	RP-A1	1024 (*3)	--(*3)
			RP-C, RP-D	2000 (*3)	
			RP-C6, RP-D6, RP-CV, RP-DV	2000	2000
GR2000-10H	64MB, 128MB, 192MB	1024	RP-A1, RP-C RP-D	1024 (*3)	--(*3)
			RP-C6, RP-D6, RP-CV, RP-DV,	1024	1024
	256MB or more	10000	RP-A1	1024 (*3)	--(*3)
			RP-C, RP-D	2000 (*3)	
			RP-C6, RP-D6, RP-CV, RP-DV,	2000	2000
GR2000-20H	64MB, 128MB, 192MB	1024	RP-A1, RP-C, RP-D	1024 (*3)	--(*3)
			RP-C6, RP-D6, RP-CV, RP-DV,	1024	1024
	256MB or more	10000	RP-A1	1024(*3)	--(*3)
			RP-C, RP-D	2000 (*3)	
			RP-C6, RP-D6, RP-CV, RP-DV,	2000	2000
GR2000-1B GR2000-2B GR2000-2B+	128MB	1000	--	1000	1000
	256MB	2000	--	2000	2000
GR2000-BH	512MB, 768MB, 1GB	2000	--	2000	2000

**1: This indicates the total value of filter and QoS entries.*
**2: The number of entries in an IPv6 filter is 256 per router and 16 per interface. IPv6 Qos cannot be set.*
**3: Cannot be set IPv6 filter or IPv6 QoS in RP-A1, RP-C and RP-D.*

Downloaded from www.Manualslib.com manuals search engine

1.1.5 *flow filter* (IPv4)

Input Form

Setting and changing the global information by each input/output interface.

```
[set] flow filter <Interface Name> {in | out} [-disable]
```

Setting and changing the flow information.

```
[set] flow filter <Interface Name> {in | out} [-disable] list <List No.>
[Flow detecting condition]
[-action
     [{ -forward | -drop | -policy <Interface Name> <IP Address>
     | -policy_group <policy-Group-Name> |
      -replace_dscp <DSCP_Value> | -index <No.> }]]
```

[Flow detecting condition]

1. When all high order protocol is target.

   ```
   ip <IP_Source> <IP_Destination> [{dscp <DSCP_Value> | precedence
   <precedence_Value>}]
   [{upper| lower} <Length>] [vlan <VLAN ID>]
   ```

2. When the high order protocol is other than TCP, UDP, ICMP and IGMP.

   ```
   <protocol No.> <IP_Source> <IP_Destination> [{dscp <DSCP_Value> |
   precedence <precedence_Value>}]
   [{upper| lower} <Length>]
   ```

3. When the high order protocol is TCP.

   ```
   tcp <IP_Source> [<Port_Source>] <IP_Destination> [<Port_Destination>]
   [ack] [syn] [{dscp <DSCP_Value> | precedence <precedence_Value>}]
   [{upper| lower} <Length>]
   ```

4. When the high order protocol is UDP.

   ```
   udp <IP_Source> [<Port_Source>] <IP_Destination> [<Port_Destination>]
   [{dscp <DSCP_Value> | precedence <precedence_Value>}] [{upper| lower}
   <Length>]
   ```

5. When the high order protocol is ICMP.

   ```
   icmp <IP_Source> <IP_Destination> [<ICMP_Type> [<ICMP_Code>]] [{dscp
   <DSCP_Value> | precedence <precedence_Value>}]
   [{upper| lower} <Length>]
   ```

6. When the high order protocol is IGMP.

   ```
   igmp <IP_Source> <IP_Destination> [<IGMP_Type>] [{dscp <DSCP_Value> |
   precedence <precedence_Value>}]
   [{upper| lower} <Length>]
   ```

   Note 1: Enter the operation designation after [flow detection conditions] when setting or changing both [flow detection conditions] and the operation designation below parameter action simultaneously.

   Note 2: If the parameters in the "flow detecting condition" and the operation designation are to be changed, input all the setting contents again.

Changing only the operation designation.

```
[set] flow filter <Interface Name> {in | out} list <List No.> -action
[{ -forward | -drop | -policy <Interface Name> <IP Address>
| -policy_group <policy-Group-Name> | -replace_dscp <DSCP_Value>
| -index <No.> }]
```


Downloaded from www.Manualslib.com manuals search engine

Deletion of the information

```
delete flow filter <Interface Name> {in | out} [list <List No.>]
```

Indication of the information

```
show flow filter [<Interface Name> [{in | out} [list <List No.>]]]
```

Indication of a blank list number in the specified range

```
show flow filter <Interface Name> {in | out} [list <List No.>-<List No.>]
free
```

Indication of top blank list number in the specified range

```
show flow filter <Interface Name> {in | out} [list <List No.>-<List No.>]
free min_no
```

Parameter

Parameters that can be set for each RP type have been determined. The list of parameters that can be set for each RP type using IPv4 filter flow information is shown in Table 1-21 List of Parameters that Can Be Set for Each RP Type Using IPv4 Filter Flow Information.

Downloaded from www.Manualslib.com manuals search engine

Table 1-21 List of Parameters that Can Be Set for Each RP Type Using IPv4 Filter Flow Information

Item		Parameter	RP-A1		RP-C, RP-D		RP-C6, RP-D6 RP-CV, RP-DV GR2000-1B, GR2000-2B, GR2000-2B+, GR2000-BH	
Main item	Sub-item		Input side	Output side	Input side	Output side	Input side	Output side
Flow detection conditions	All protocol IPs	ip	√	√	√	√	√	√
	Protocol number	<protocol No.>	√	√	√	√	√	√
	Protocol TCP	tcp	√	√	√	√	√	√
	Protocol UDP	udp	√	√	√	√	√	√
	Protocol ICMP	icmp	√	√	√	√	√	√
	Protocol IGMP	igmp	√	√	√	√	√	√
	Source IP address	<IP_Source>	√	√	√	√	√	√
	Destination IP address	<IP_Destination>	√	√	√	√	√	√
	DSCP	dscp <DSCP_Value>	√	√	√	√	√	√
	precedence	precedence <precedence_Value>	√	√	√	√	√	√
	IP user data length	{upper | lower} <Length>	√	√	√	√	√	√
	Source port number	<Port_Source>	√	√	√	√	√	√
	Destination port number	<Port_Destination>	√	√	√	√	√	√
	ack flag	ack	√	√	√	√	√	√
	syn flag	syn	√	√	√	√	√	√
	ICMP type	<ICMP_Type>	√	√	√	√	√	√
	ICMP code	<ICMP_Code>	√	√	√	√	√	√
	IGMP type	<IGMP_Type>	–	–	√	√	√	√
	VLAN ID	vlan <VLAN_ID>	–	–	√	–	√	–
Designation of operation	Relay	forward	√	√	√	√	√	√
	Discard	drop	√	√	√	√	√	√
	Policy routing	policy <Interface Name> <IP Address>	√	–	√	–	√	–
	Policy routing loop	policy_group <policy-Group-Name>	√	–	√	–	√	–
	DSCP	replace_dscp <DSCP_Value>	√	√(*1)	√	√(*1)	√	√(*1)
	Connection branch	index <No.>	–	√	–	√	–	√

√: Can be set.
-: Cannot be set.
**1: Cannot be set for multi-cast.*

<Interface Name>

The subject interface name set in the IP information or the IP-address information is designated. (The IP information or IP-address information should have been set before inputting this command.) The RM Ethernet is not supported. For details, refer to Table 1-5.

Default: No default is possible.

Downloaded from www.Manualslib.com manuals search engine

{ in | out }

Inbound/Outbound is designated. Either one or both of the Inbound/Outbound can be set simultaneously.

in :Inbound (Designation of frame input side)

out:Outbound (Designation of frame output side)

Default: No default is possible.

[-disable]

The flow control is nullified by each input/output interface.

Default: No default is possible.

list <List No.>

The list numbers are designated.

Default: Default is possible only for the case of indication. All the lists are indicated at default.

Range of value: IPv4 filter list: 1 to 20000 (decimal)

[list <List No.>-list <list No.>]

Description: Specifies the range of a list number. This parameter can be specified only when a blank list number is displayed.

Default: The range of the list number to be displayed corresponds to all list numbers.

Range of value: IPv4 filter list: 1 to 20000 (Decimal)
IPv6 filter list: 40001 to 60000 (Decimal)

free

Description: Displays the blank list number.

Default: Cannot be omitted when the blank list number is displayed.

min_no

Description: Displays the top blank list number in the specified range.

Default: Cannot be omitted when the top list number of a blank list number is displayed.

- Flow detecting condition parameter

{ ip | <protocol No.> | tcp | udp | icmp | igmp }

Description: The high-order protocol numbers or protocol names are designated. If all protocols are taken as the object, IP is designated.

In case of IPv4 filter list, icmp6 cannot be designated. In case of IPv6 filter list, icmp and igmp cannot be designated.

Default: No default is possible.

Range of value: 0 to 255 (decimal). (Please refer to Table 1-22.)

Downloaded from www.Manualslib.com manuals search engine

However, in case of the IPv6 filter list, the protocol number showing the IPv6 option header cannot be designated. Specifically, the numbers are 0 (relaying point option header), 43 (route control header), 44 (fragment header), 50 (code payload header), 51 (certification header), 59 (no next header), and 60 (ending point option).

Table 1-22 General Protocol Number

Protocol No.	Protocol
1	ICMP
6	TCP
8	EGP
17	UDP
88	IGRP
89	OSPF

<IP_Source>

Transmitter IPv4 address is designated.

If address to be designated is one: nnn.nnn.nnn.nnn

If address is designated by range: nnn.nnn.nnn.nnn-nnn.nnn.nnn.nnn

If designated by sub-net mask length: nnn.nnn.nnn.nnn/aa

If all IPv4 addresses are designated: any

Default: No default is possible.

Range of value: IPv4 address (nnn.nnn.nnn.nnn): 0.0.0.0-255.255.255.255
Sub-net mask length (aa): 0-32

<IP_Destination>

Destination IPv4 address is designated.

If address to be designated is one: nnn.nnn.nnn.nnn

If address is designated by range: nnn.nnn.nnn.nnn-nnn.nnn.nnn.nnn

If designated by sub-net mask length: nnn.nnn.nnn.nnn/aa

If all IPv4 addresses are designated:any

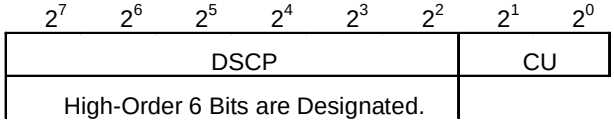
Default: No default is possible.

Range of value: IPv4 address (nnn.nnn.nnn.nnn):0.0.0.0-255.255.255.255

Sub-net mask length (aa): 0-32

[dscp <DSCP_Value>]

This parameter specifies the DSCP value that is the upper six bits of a TOS field. The DSCP value is compared with the upper six bits of a TOS field in a receive packet. The lower two bits of a TOS field are ignored.



DSCP (Differentiated Services Code Point), CU (Current Unused)

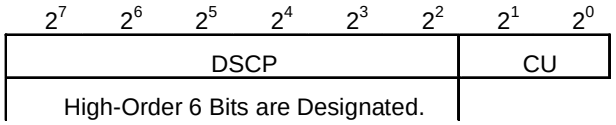
Downloaded from www.Manualslib.com manuals search engine

Default: None (DSCP values are not included in the flow detecting condition.)

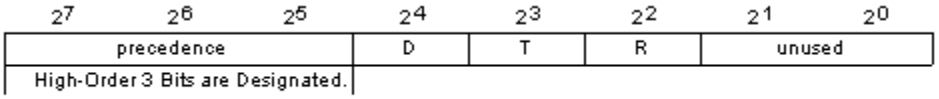
Range of value: 0 to 63 (decimal).

`[precedence <precedence_Value>]`

This parameter specifies precedence value, which is the upper 3 bits of the ToS field. This is compared to the upper 3 bits of the ToS field of sent/received packets. The lower 5 bits of the ToS field are ignored.



DSCP (Differentiated Services Code Point), CU (Current Unused)



D(Delay), T(Troughput), R(Reliability)

Default: None (precedence values are not included in the detecting condition)

Range of value: 0 - 7 (decimal)

`[{ upper | lower } <Length>]`

Description: Upper limit or lower limit of the IP user data length are designated (Table 1-23).

-upper: Upper limit of the IP user data length is designated.

-lower: Lower limit of the IP user data length is designated.

default: None (TOS values are not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal).

Table 1-23 Relationship between Upper and Lower IP User Data Length Llimits and IP User Data Length

Upper and Lower Limits Designation	Relationship between A (Packet Value): (Total Length) - (Header Length) and B (IP user data length designated in constituting definition information)	Result
-upper	A ≤ B	Agreed
-upper	A > B	Disagreed
-lower	A ≥ B	Agreed
-lower	A < B	Disagreed

Downloaded from www.Manualslib.com manuals search engine

[vlan <VLAN ID>]

Description: Sets the VLAN ID of tag-VLAN.
The list information that sets this parameter should be set in (Inbound) and specified as the flow detection conditions on the input side.

Default: Undefined. (VLAN ID is not contained in the flow detection conditions.)

Range of value: 1 to 4095 (This parameter is valid only in RP-C and RP-D.)

[<Port_Source>]

Transmitter port numbers are designated.

If port number to be designated is one: nnnnn

If port number is designated by range:nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-24.)

[<Port_Destination>]

Destination port numbers are designated.

If port number to be designated is one: nnnnn

If port number is designated by range:nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-24.)

Table 1-24 General port number

Port Number (Decimal)	Name
20/tcp	File Transfer [Default Data]
21/tcp	File Transfer [Control]
22/tcp	Secure Shell Login
23/tcp	Telnet
25/tcp	Simple Mail Transfer
53/tcp 53/udp	Domain Name Server
80/tcp	World Wide Web HTTP
110/tcp 10/udp	Post Office Protocol - Version 3
161/udp	SNMP

[ack]

TCP single-direction communication permit (having one ACK flag) is designated.(note1)

Default: None (the ACK flag is not included in the flow detecting condition.)

Range of value: None

[syn]

Virtual circuit establishment permit (having one SYN fla) is designated.(Note1)

Downloaded from www.Manualslib.com manuals search engine

Default: None (the SYN flag is not included in the flow detecting condition.)

Range of value: None

[<ICMP_Type>]

ICMP type is designated.

Default: None (the ICMP type is not included in the flow detecting condition.)

Range of value: 0 to 255 (decimal). (Please refer to Table 1-25.)

[<ICMP_Code>]

ICMP code is designated.

Default: None (the ICMP code is not included in the flow detecting condition.)

Range of value: 0 to 255 (decimal). (Please refer to Table 1-25.)

Table 1-25 General ICMP Type and Code Nnumber

Type	Name	Code
0	Echo Reply	0
3	Destination Unreachable	0-12
4	Source Quench	0
5	Redirect	0-3
8	Echo	0
11	Time Exceeded	0-1
12	Parameter Problem	0
13	Timestamp	0
14	Timestamp Reply	0
17	Address Mask Request	0
18	Address Mask Reply	0

[<IGMP_type>]

ICMP type is designated.

Default: None (the ICMP type is not included in the flow detecting condition.)

Range of value: 0 to 255 (decimal). (Please refer to Table 1-26.)

Table 1-26 General ICMP Type Number

Type	Name
17	Membership Query
18	Version 1 Membership Report
19	DVMRP protocol
22	Version 2 Membership Report
23	Version 2 Leave Group
34	Version 3 Membership Report

Downloaded from www.Manualslib.com manuals search engine

- Operation Parameter

[-action]

If the operation parameter is either set or changed, please be sure to set this parameter at the head of the whole operation parameter.

Default: None (No default is possible when designating the operation.)

Range of value: None

[{-forward | -drop}]

Operation which agrees with the flow detecting condition is designated.

-forward:The agreed package is relayed.

-drop :The agreed packet is discarded.

Default: -forward

Range of value: None

[-policy <Interface Name> <IP Address>]

The policy routing function is made effective. When relaying a packet that agrees with the filter condition, the packet is transmitted to the output destination designated by this option. Designate "in" (Inbound) for the list information that has set the policy routing, as the flow control of the reception side.

<Interface Name>: Designate the interface name of the output destination (the interface name set in the IP information). (Refer toTable 1-27.))

Table 1-27 List of Interfaces Supporting Flow Control

Interface Name	Availability of Support
<Line Name>	√
RmEthernet	---
<DLCI Name>	√
<VC Name>	√
<Group Name>	√
<Timeslot Name>	√
<Peer Name>	√
<Tunnel Name>	---
<VLAN Name>	---(1*)
<Session Name>	--- (1*)

√: Setting possible.
-: Setting impossible
**1: VLAN line and PPOoE session are not supported.*

<IP Address>:Designate the next hop IPv4 address.

Default: forward

Range of value: <IP Address>: Set the IPv4 addresses shown below:

Class A : 1.0.0.1-126.255.255.254

Class B : 128.1.0.1-191.254.255.254

Class C : 192.0.1.1-233.255.254.254

Downloaded from www.Manualslib.com manuals search engine

No setting is possible for the IPv4 addresses of 127.0.0.0-127.255.255.255, and IPv4 addresses of class D [224.0.0.0-239.255.255.255) and broadcast address (in which net ID or host ID is a binary number, and all is one or zero).

`[-policy_group <policy-Group-Name>]`

The policy group name designated in the policy-group is designated. When relaying a packet that agrees with the filter condition, the packet is transmitted to the route of the highest priority among the output destinations registered in the policy group designated by this option. Designate in (Inbound) for the list information that has set the policy routing, as the flow control of the reception side.

Default: -forward

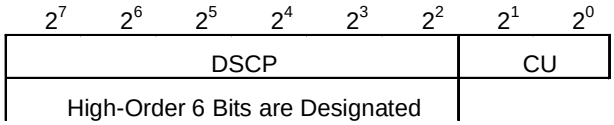
Range of value: The policy group name designated in the policy-group information.

Default: -forward

Range of value: -replace_tos <TOS_Value>:0-255(decimal) (Note 1, 2)

`[-replace_dscp <DSCP_Value>]`

This parameter enables the function that rewrites a DSCP value. It rewrites the DSCP value that is the upper six bits of a TOS field. The lower two bits of a TOS field are not rewritten. On the output side, do not specify this parameter to multicast packets. It cannot be set in the tunnel interface.



DSCP (Differentiated Services Code Point), CU (Current Unused)

Default: -forward

Range of value: -replace_dscp <DSCP_Value>: 0 to 63 (decimal).

`[-index <No.>]`

Designate the connection branching index numbers (indexes designated by the DLCI group information or the Vc-Group information). When relaying a packet that agrees with the flow detecting condition, DLCI/VC designated in the group is selected and transmitted. Designate "out" (Outbound) for the list information that has set the connection branching index number, as the flow control of the output side. (This parameter is effective only for RP-A and RP-D.) It cannot be set in the tunnel interface.

Default: -forward

Range of value: 0 to 7.

Note: Define the filtering according to the *GR2000 Configuration Settings (universal CLI)* manual when the IPv4 packets shown in the table below are filtered under the ACK/SYN flag conditions of a TCP header. The filtering of the IPv4 packets shown in the table below that is performed under the ACK/SYN flag conditions of a TCP header is limited when IPv4 packets are used in a way except as described above. The IPv4 packets cannot be properly filtered even if *ack* and *syn* parameters are set to the filter flow information.

Downloaded from www.Manualslib.com manuals search engine

Table 1-28 Packet Type in which the Filtering Based on the Flag (ACK and SYN) Conditions of TCP Header Is Limited in Use

Packet Type	Limited Filtering Item
IPv4 packet generated by this router	• IPv4 packets do not match the filter list, to which "-ack_check" or "-syn_check" is set, in conditions. In other words, both ACK and SYN flags are searched for filtering as if packet 0 were input.
Packet applied to the conditions below among the IPv4 packets relayed by this router: (1) Packet with option (IP header)	The same as described above.
Packet applied to the conditions below among the IPv4 packets relayed by this router: (2) Packet requiring fragmentation (3) Packet requiring redirection (4) Packet in which ARP has not been solved	• The packets to be discarded are properly discarded when they conform to the filtering conditions. • The packets to be relayed do not match the filter list, to which "-ack_check" or "-syn_check" is set, in conditions when they conform to the filtering conditions. In other words, both ACK and SYN flags are searched for filtering as if packet 0 were input.

Input Examples

1. Setting the filter flow information

   - Designation of relay and/or discard
     Designate relaying the packets with the transmitter IP address being 10.10.10.2, the high-order protocol being TCP and the destination port number being 23 (telnet). Designate other packets to be discarded.

```
(config)#  flow filter Tokyo out list 1 tcp 10.10.10.2 any 23 -action
-forward
(config)#  flow filter Tokyo out list 2000 ip any any -action -drop
(config)#  flow -yes
(config)#  show flow
flow yes {
        filter Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action forward;
                list 2000 ip any any action drop;
        };
};
(config)#
```

   - Designation of policy routing
     Output packets with transmitter IPv4 addresses being 10.10.10.2 from the interface with the interface name of Osaka making the next hop address 10.10.20.20.

```
(config)#  flow filter Tokyo in list 1 ip any 10.10.10.2 action -policy
Osaka 10.10
.20.20
(config)#  flow -yes
(config)#  show flow
flow yes {
        filter Tokyo in {
                list 1 ip 10.10.10.2 any action policy Osaka 10.10.20.20;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Designation of policy routing group:
  Output a packet with the transmitter IPv4 address being 10.10.10.2 by selecting one list from the list registered in the group whose policy routing group name is RedGroup.

```
(config)#  flow filter Tokyo in list 1 ip any 10.10.10.2 -action
-policy_group RedGr
oup
(config)#  flow -yes
(config)#  show flow
flow yes {
        filter Tokyo in {
                list 1 ip any 10.10.10.2 action policy_group Redgroup;
        };
};
(config)#
```

2. Insertion of lists:
   - Insert the list number 3 between the list numbers 1 and 5.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out list 3 tcp any any -action -forward
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 3 tcp any any action forward;
                list 5 ip any any action drop;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Nullification of filter flow information by each input/output interface:
   Nullify the filter flow control of the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out -disable
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out disable {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```

4. Change of parameters:
   - Change of parameters for flow detecting condition and the operation designation.
     Change the parameters for flow detecting condition and the operation Designation whose list number is one.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out list 1 tcp 10.10.10.2 any 23 -action
-forward
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action forward;
                list 5 ip any any action drop;
        };
};
```


Downloaded from www.Manualslib.com manuals search engine

- Change of parameter only for the operation designation:
  Change the parameter for the list number one from relay (forward) to discard (drop).

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out list 1 -action -drop
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action drop;
                list 5 ip any any action drop;
        };
};
(config)#
```

5. Deletion of filter flow information:
   - Deletion in input/output interface unit
     Delete the filter flow information of the output interface, Tokyo.

```
(config)#  show flow filter
flow yes {
        filter Tokyo in {
                list 1 ip 10.10.10.2 any action policy Osaka 10.10.20.20;
        };
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  delete flow filter Tokyo out
(config)#  show flow filter
flow yes {
        filter Tokyo in {
                list 1 ip 10.10.10.2 any action policy Osaka 10.10.20.20;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Deletion in list unit:
  Delete the list number one for the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  delete flow filter Tokyo out list 1
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```

- Deletion of operation designation parameter:
  Delete the operation designation in the list number one of the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
        };
};
(config)#  delete flow filter Tokyo out list 1 --action
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1;
                list 5 ip any any action drop;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Indication of filter flow information:
   - Indication of all input/output interfaces
     Indicate the filter flow information of all input/output interfaces.

```
(config)#  show flow filter
flow yes {
        filter Tokyo in {
                list 1 ip 10.10.10.2 any action policy Osaka 10.10.20.20;
        };
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```

   - Indication in input/output interface unit:
     Indicate the flow information of the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 1 ip any 10.10.10.1 action forward;
                list 5 ip any any action drop;
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```

   - Indication in list unit:
     Indicate the flow information of the list number 5 of the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out list 5
flow yes {
        filter Tokyo out {
                list 5 ip any any action drop;
        };
};
(config)#
```

7. Display of blank list number:
   - Display of all blank list numbers
     Display all blank list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in free
Free number: 5,7,15-20000
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Display of blank list number in the specified range:
  Display all blank list numbers in the range in which the list number is 1 to 100 on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in list 1-100 free
Free number: 5,7,15-100
(config)#
```

- Display of top blank list number in all list numbers:
  Display the top blank list number in the list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in free min_no
Free number: 5
(config)#
```

- Display of top blank list number in the specified range:
  Display the top blank list number in the range in which the list number is 51 to 100 on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in list 51-100 free min_no
Free number: 51
(config)#
```

Related Commands

flow, flow qos, filter, filter-list, qos, qos-ip-list, qos-tos-map, nat, nat inside interface, nat outside interface

Related Information

None

Precautions

1. The filter flow is determined in the order of the list number designated in the input/output interface of the filter IP flow information (the indication order when show flow filter is executed).
2. This command cannot be set when setting the filter-list (filter list information) or qos-ip-list (QoS IP frame condition information). Delete all of the filter-list and qos-ip-list before setting this command.
3. The input form for the filter flow information includes two forms: the flow filter constituting definition information and the filter-list, filter-group and filter-interface constituting definition information. Features by each input form are shown in Table 1-9.
4. Flow information consumes 101 entries in each RP when address conversion (nat) is set. Therefore, when address conversion (nat) is set, the maximum entry count is decreased by 101 per RP capable of flow information definition.

Downloaded from www.Manualslib.com manuals search engine

1.1.6 *flow filter* (IPv6) [ROUTE-OS6]

Input Format

Setting

- Setting and changing the global information by each input/output interface.

  [set] flow filter <Interface Name> {in | out} [-disable]

- Setting and changing the flow information.

```
[set] flow filter <Interface Name> {in | out} [-disable] list <List No.>
{Flow detecting condition}
[-action
[{ -forward | -drop | -policy <Interface Name> <IP Address> |
-replace_dscp <DSCP_Value> | -index <No.>}][ -scan_extension]
```

Flow cetecting condition

1. When the high order protocol is other than TCP, UDP and IGMPv6.
   ```
   {ip | <protocol No.>} <IPv6_Source> <IPv6_Destination> [{dscp
   <DSCP_Value> | precedence <precedence_Value>}] [{upper| lower} <Length>]
   ```
2. When the high order protocol is TCP.
   ```
   tcp <IPv6_Source> [<Port_Source>] <IPv6_Destination> [<Port_Destination>]
   [ack] [syn] [{dscp <DSCP_Value> | precedence <precedence_Value>}]
   [{upper| lower} <Length>]
   ```
3. When the high order protocol is UDP.
   ```
   udp <IPv6_Source> [<Port_Source>] <IPv6_Destination> [<Port_Destination>]
   [{dscp <DSCP_Value> | precedence <precedence_Value>}] [{upper| lower}
   <Length>]
   ```
4. When the high order protocol is ICMPv6.
   ```
   icmp6 <IPv6_Source> <IPv6_Destination> [<ICMPv6_Type> [<ICMPv6_Code>]]
   [{dscp <DSCP_Value> | precedence <precedence_Value>}] [{upper | lower}
   <Length>]
   ```

Note: 1: If the "flow detecting condition" and the operation designation (*1) are set or changed simultaneously, input the operation designation after the "detecting condition2.

Note: 2: If the parameters in the "flow detecting condition" and the operation designation are to be changed, input all the setting contents again.

Changing only the operation designation.

```
[set] flow filter <Interface Name> {in | out} list <List No.> -action [{
-forward | -drop
| -policy <Interface Name> <IP Address> | -replace_dscp <DSCP_Value> |
-index <No.> | scan_extension}]
```

Deletion of the information

```
delete flow filter <Interface Name> {in | out} [list <List No.>]
```

Indication of the information

```
show flow filter [<Interface Name> [{in | out} [list <List No.>]]]
```

Indication of a blank list number in the specified range

```
show flow filter <Interface Name> {in | out} [list <List No.>-<List No.>]
free
```


Downloaded from www.Manualslib.com manuals search engine

Indication of top blank list number in the specified range

```
show flow filter <Interface Name> {in | out} [list <List No.>-<List No.>]
free min_no
```

Parameters

Parameters that can be set for each RP type have been determined. The list of parameters that can be set for each RP type using IPv6 filter flow information is shown in Table 1-29 List of Parameters that Can Be Set for Each RP Type Using IPv6 Filter Flow Information.

Table 1-29 List of Parameters that Can Be Set for Each RP Type Using IPv6 Filter Flow Information

Item		Parameter	RP-A1 RP-C, RP-D		RP-C6, RP-D6 GR2000-1B, GR2000-2B	
Main Item	Sub-Item		Input Side	Output Side	Input Side	Output Side
Flow detection conditions	All protocol IPs	ip	x	x	√	√
	Protocol number	<protocol No.>	x	x	√	√
	Protocol TCP	tcp	x	x	√	√
	Protocol UDP	udp	x	x	√	√
	Protocol ICMP	icmp6	x	x	√	√
	Source IP address	<IP_Source>	x	x	√	√
	Destination IP address	<IP_Destination>	x	x	√	√
	DSCP	dscp <DSCP_Value>	x	x	√	√
	precedence	precedence <precedence_Value>	--	--	√	√
	IP user data length	{upper | lower} <Length>	x	x	√	√
	Source port number	<Port_Source>	x	x	√	√
	Destination port number	<Port_Destination>	x	x	√	√
	ack flag	ack	x	x	√	√
	syn flag	syn	x	x	√	√
	ICMP6 type	<ICMPv6_Type>	x	x	√	√
	ICMP6 code	<ICMPv6_Code>	x	x	√	√
Designation of operation	Relay	forward	x	x	√	√
	Discard	drop	x	x	√	√
	Policy routing	policy <Interface Name> <IP Address>	–	–	√	–
	DSCP	replace_DSCP <DSCP_Value>	–	–	√	√(*1)
	Connection branch	index <No.>	–	–	–	√
	Extended header additional function	scan_extension	–	–	√	√

√: Can be set.
-: Cannot be set.
x: Can be set when RP-C6, RP-D6, RP-CV, and RP-DV are not installed in this router.
**1: Cannot be set for multi-cast.*

Downloaded from www.Manualslib.com manuals search engine

<Interface Name>

Description: The subject interface name set in the IP information or the IP-address information is designated. (The IP information or IP-address information should have been set before inputting this command.) The RM Ethernet is not supported. For details, refer to Table 1-5.

Default: No default is possible.

{in | out }

Description: Inbound/Outbound is designated. Either one or both of the Inbound/Outbound can be set simultaneously.
in :Inbound (designation on the frame input side)
out:Outbound (designation on the frame output side)

Default: No default is possible.

[-disable]

Description: The flow control is nullified by each input/output interface.

Default: No default is possible.

list <List No.>

Description: The list numbers are designated.

Default: Default is possible only for the case of indication. All the lists are indicated at default.

Range of value: IPv6 filter list: 40001 to 60000 (decimal)

[list <List No.>-list <list No.>]

Description: Specifies the range of a list number. This parameter can be specified only when a blank list number is displayed.

Default: The range of the list number to be displayed corresponds to all list numbers.

Range of value: IPv4 filter list: 1 to 20000 (decimal)
IPv6 filter list: 40001 to 60000 (decimal)

free

Description: Displays the blank list number.

Default: Cannot be omitted when the blank list number is displayed.

min_no

Description: Displays the top blank list number in the specified range.

Default: Cannot be omitted when the top list number of a blank list number is displayed.

- Flow detecting condition parameter

{ip |<protocolNo.>| tcp|udp|icmp6}

Description: The high-order protocol numbers or protocol names are designated. If all protocols are taken as the object, IP is designated.

Downloaded from www.Manualslib.com manuals search engine

Default: No default is possible.

Range of value: 0 to 255 (decimal). (Please refer to Table 1-30.)

However, in case of the IPv6 filter list, the protocol number showing the IPv6 option header cannot be designated. Specifically, the numbers are 0 (relaying point option header), 43 (route control header), 44 (fragment header), and 60 (ending point option).

Table 1-30 General Protocol Number

Protocol No.	Protocol
1	ICMP
6	TCP
8	EDP
17	UDP
58	ICMPv6
88	IGRP
89	OSPF

<IPv6_Source>

Transmitter IPv6 address is designated.

If address to be designated is one:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If address is designated by range:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn -
nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If designated by sub-net prefix length:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/aaa

If all IPv6 addresses are designated: any

Default: No default is possible.

Range of value: IPv6 address (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn): 0:0:0:0:0:0:0:0-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Prefix length (aaa): 0-128

<IPv6_Destination>

Designated filter conditions by Transmitter IPv6 address.

If address to be designated is

one:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If address is designated by range

:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn -nnnn:
nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If designated by sub-net mask length:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/aaa

If all IPv6 addresses are designated: any

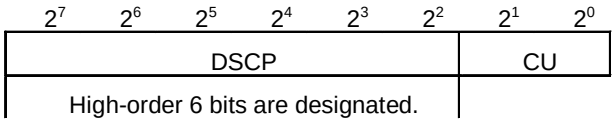
Default: No default is possible.

Downloaded from www.Manualslib.com manuals search engine

Range of value: IPv6 address
(nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):
0:0:0:0:0:0:0-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Sub-net mask length (aaa): 0-128

`[dscp <DSCP_Value>]`

This parameter specifies the DSCP value that is the upper six bits of a Traffic class field. The DSCP value is compared with the upper six bits of a Traffic class field in a receive packet. The lower two bits of a TOS field are ignored.



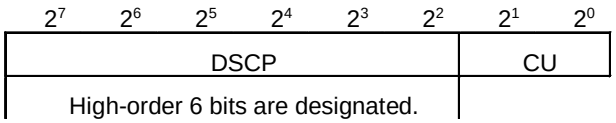
DSCP(Differentiated Services Code Point), CU(Current Unused)

Default: None (DSCP values are not included in the flow detecting condition.)

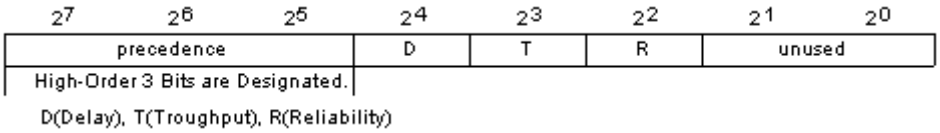
Range of value: 0 to 63 (decimal).

`[precedence <precedence_Value>]`

This parameter specifies precedence value, which is the upper 3 bits of the ToS field. This is compared to the upper 3 bits of the ToS field of sent/received packets. The lower 5 bits of the ToS field are ignored.



DSCP(Differentiated Services Code Point), CU(Current Unused)



Default: None (precedence values are not included in the detecting condition)

Range of value: 0 - 7 (decimal)

`[{ upper | lower } <Length>]`

Description: Upper limit or lower limit of the IP user data length are designated.

-upper:Upper limit of the IP user data length is designated.

-lower:Lower limit of the IP user data length is designated.

Default: None (TOS values are not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal).

Downloaded from www.Manualslib.com manuals search engine

Table 1-31 Relationship Between Upper and Lower IP User Data Length Limits and IP User Data Length

Upper and Lower Limits Designation	Relationship between A (packet value) : (Total Length) - (Header Length)) and B (IP user data length designated in constituting definition information)	Result
-upper	A ≦ B	Agreed.
-upper	A > B	Disagreed.
-lower	A ≧ B	Agreed
-lower	A < B	Disagreed.

[<Port_Source>]

Transmitter port numbers are designated.

If port number to be designated is one: nnnnn

If port number is designated by range: nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-32.)

[<Port_Destination>]

Destination port numbers are designated.

If port number to be designated is one: nnnnn

If port number is designated by range: nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-32.)

Table 1-32 General Port Number

Protocol No.	Protocol
20/tcp	File Transfer [Default Data]
21/tcp	File Transfer [Control]
22/tcp	Secure Shell Login
23/tcp	Telnet
25/tcp	Simple Mail Transfer
53/tcp 53/udp	Domain Name Server
80/tcp	World Wide Web HTTP
110/tcp 110/udp	Post Office Protocol - Version 3
161/udp	SNMP

[ack]

TCP single-direction communication permit (having one ACK flag) is designated.

Default: None (the ACK flag is not included in the flow detecting condition.)

Range of value: None

Downloaded from www.Manualslib.com manuals search engine

[syn]

Virtual circuit establishment permit (having one SYN flag) is designated.

Default: None (the SYN flag is not included in the flow detecting condition.)

Range of value: None

[<ICMPv6_Type>]

ICMP type is designated.

Default: None (the ICMPv6 type is not included in the flow detecting condition.)

Range of value: 0 to 255 (decimal). (Please refer to Table 1-33)

[<ICMPv6_Code>]

ICMPv6 code is designated.

Default: None (the ICMPv6 code is not included in the flow detecting condition.)

Range of value: 0 to 255 (decimal). (Please refer to Table 1-33.)

Table 1-33 General ICMPv6 Type and Code Number

Type	Name	Code
1	Destination Unreachable	0 - 4
2	Packet Too Big	0
3	Time Exceeded	0 - 1
4	Parameter Problem	0 - 2
128	Echo	0
129	Echo Reply	0
130	Multicast Listener Query	0
131	Multicast Listener Report	0
132	Multicast Listener Done	0
133	Router Solicitation (NDP)	0
134	Router Advertusement (NDP)	0
135	Neighbor Solicitation (NDP)	0
136	Neighbor Advertusement (NDP)	0
137	Redirect (NDP)	0

Operation Parameters

[-action]

If the operation parameter is either set or changed, please be sure to set this parameter at the head of the whole operation parameter.

Default: None (No default is possible when designating the operation.)

Range of value: None

[{-forward | -drop}]

Operation which agrees with the flow detecting condition is designated.

-forward: The agreed package is relayed.

Downloaded from www.Manualslib.com manuals search engine

-drop: The agreed packet is discarded.

Default: -forward

Range of value: None

[-policy <Interface Name> <IP Address>]

This parameter enables the function of policy routing. Packets are transmitted to the output destination specified using this option when relaying the packets that coincide with filter conditions. For the list information that sets policy routing, specify in (Inbound) and then specify it as the flow control on the receive side.

<Interface Name>:

Specifies the interface name at the output destination (the interface name set using ip information) (refer toTable 1-34).

Table 1-34 List of Interfaces that Support Flow Control

Interface Name	Availability of Support
<Line Name>	√
RmEthernet	---
<DLCI Name>	√
<VC Name>	√
<Group Name>	√
<Timeslot Name>	√
<Peer Name>	√
<Tunnel Name>	---
<VLAN Name>	---(1*)
<Session Name>	--- (1*)

√: Setting possible.
-: Setting impossible
**1: VLAN line and PPOoE session are not supported.*

<IP Address>:

Specifies the next hop IPv6 address.

Default: -forward

Range of value: <IP Address>: Set the IPv6 address described below.
IPv6 address
:(nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):
0:0:0:0:0:0:0-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[-index <No.>]

Designate the connection branching index numbers (indexes designated by the DLCI group information or the Vc-Group information). When relaying a packet that agrees with the flow detecting condition, DLCI/VC designated in the group is selected and transmitted. Designate "out" (Outbound) for the list information that has set the connection branching index number, as the flow control of the transmission side. It cannot be set in the tunnel interface.

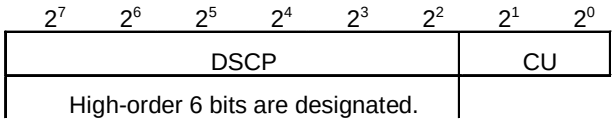
Default: -forward

Range of value: 0 to 7.

Downloaded from www.Manualslib.com manuals search engine

[-replace_dscp <DSCP_Value>]

This parameter enables the function that rewrites a DSCP value. It rewrites the DSCP value that is the upper six bits of a TOS field. The lower two bits of a TOS field are not rewritten. On the output side, do not specify this parameter to multicast packets. It cannot be set in the tunnel interface.



DSCP(Differentiated Services Code Point), CU(Current Unused)

Default: -forward

Range of value: -replace_tos <DSCP_Value>:0-63(decimal)

[-sacn_extension]

This parameter enables the filtering function that sets four-layer information (TCP, UPD, or ICMPv6) to the packet with an extended header as conditions using RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B, GR2000-2B, GR2000-2B+ or GR2000-BH.

The protocol parameter that can be jointly used with this parameter is only ip. The operating parameter that can be jointly used with this parameter is only forward and drop.

Input Examples

1. Setting the filter flow information:
   Designation of relay and/or discard(IPv6 filter)
   Designate relaying the IPv6 packets with the transmitter IPv6 address being 3ffe:501:811:ff01:1::1, the high-order protocol being TCP and the destination port number being 23 (telnet). Designate other packets to be discarded.

```
(config)#  flow filter Tokyo in list 40001 tcp 3ffe:501:811:ff00:1::1 any
23 -action -forward
(config)#  flow filter Tokyo in list 42000 ip any any -action -drop
(config)#  flow -yes
(config)#  show flow
flow yes {
        filter Tokyo in {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```

   Designation of policy routing:
   Output packets with transmitter IPv6 addresses being 3ffe:501:811:ff01:1::1 from the interface with the interface name of Osaka making the next hop address 3ffe:501:811:ff20:1::1.

Downloaded from www.Manualslib.com manuals search engine

```
(config)#  flow filter Tokyo in list 40001 ip any 3ffe:501:811:ff01:1::1
-action -policy Osaka 3ffe:501:811:ff20:1::1
(config)#  flow -yes
(config)#  show flow
flow yes {
        filter Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action policy
Osaka 3ffe:501:811:ff20:1::1;
        };
};
(config)#
```

2. Insertion of lists:
   Insert the list number 40003 between the list numbers 40001 and 42000.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out list 40003 tcp any any -action -forward
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 40003 tcp any any action forward
                list 42000 ip any any action drop;
        };
};
(config)#
```

3. Nullification of filter flow information by each input/output interface:
   Nullify the filter flow control of the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out -disable
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out disable {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Change of parameters:
   Change the parameters for flow detecting condition and the operation Designation whose list number is 40001.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip any 3ffe:501:811:ff01:1::1 action forward;
                list 40005 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out list 40001 tcp 3ffe:501:811:ff01:1::1 any
23 -action -forward
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
forward;
                list 40005 ip any any action drop;
        };
};
(config)#
```

   Change of parameter only for the operation designation:

   Change the parameter for the list number one from relay (forward) to discard (drop).

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip any 3ffe:501:811:ff01:1::1 action forward;
                list 40005 ip any any action drop;
        };
};
(config)#  flow filter Tokyo out list 40001 action drop
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action drop;
                list 40005 ip any any action drop;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

5. Deletion of filter flow information Deletion in input/output interface unit:
   Delete the filter flow information of the output interface, Tokyo.

```
(config)#  show flow filter
flow yes {
        filter Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action policy
Osaka 3ffe:501:811:ff20:1::1;
        };
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  delete flow filter Tokyo out
(config)#  show flow filter
flow yes {
        filter Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action policy
Osaka 3ffe:501:811:ff20:1::1;
        };
};
(config)#
```

Deletion in list unit:

Delete the list number 40001 for the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#  delete flow filter Tokyo out list 40001
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 42000 ip any any action drop;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Delete the operation parameter:

Delete the list number 40001 for the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip any 3ffe:501:811:ff01:1::1 action forward;
                list 40005 ip any any action drop;
        };
};
(config)#  delete flow filter Tokyo out list 40001 --action
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip any 3ffe:501:811:ff01:1::1;
                list 40005 ip any any action drop;
        };
};
(config)#
```

6. Indication of filter flow information

   Indication of all input/output interfaces

   Indicate the filter flow information of all input/output interfaces.

```
(config)#  show flow filter
flow yes {
        filter Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action policy
Osaka 3ffe:501:811:ff20:1::1;
        };
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```

Indication in list unit:

Indicate the flow information of the output interface, Tokyo.

```
(config)#  show flow filter Tokyo out
flow yes {
        filter Tokyo out {
                list 40001 ip 3ffe:501:811:ff00::0/64 any action forward;
                list 42000 ip any any action drop;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Indication in list unit

Indicate the flow information of the list number 40005 of the output interface, Tokyo.

```
(config)# show flow filter Tokyo out list 40005
flow yes {
        filter Tokyo out {
                list 40005 ip any any action drop;
        };
};
(config)#
```

7. Display of blank list number
   Display of all blank list numbers
   Display all blank list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow filter Tokyo in free
Free number(IPv4): 5,7,15-20000
Free number(IPv6): 40002-60000
(config)#
```

Display of blank list number in the specified range

Display all blank list numbers in the range in which the list number is 10001 to 40100 on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow filter Tokyo in list 40001-40100 free
Free number(IPv6): 40002-40100
(config)#
```

Display of top blank list number in all list numbers

Display the top blank list number in the list numbers on the Inbound (input) side of interface Tokyo.

```
 (config)# show flow filter Tokyo in free min_no
Free number(IPv4): 5
Free number(IPv6): 40001
(config)#
```

Display of top blank list number in the specified range

Display the top blank list number in the range in which the list number is 400051 to 40100 on the Inbound (input) side of interface Tokyo.

```
(config)# show flow filter Tokyo in list 40051-40100 free min_no
Free number(IPv6): 40051
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

flow, flow qos, filter, filter-list, qos, qos-ip-list, qos-tos-map, nat, nat inside interface, nat outside interface

Related Information

None

Precautions

1. The filter flow is determined in the order of the list number designated in the input/output interface of the filter IP flow information (the indication order when show flow filter is executed).
2. This command cannot be set when setting the filter-list (filter list information) or qos-ip-list (QoS IP frame condition information). Delete all of filter-list and qos-ip-list before setting this command.
3. Flow information consumes 101 entries in each RP when address conversion (nat) is set. Therefore, when address conversion (nat) is set, the maximum entry count is decreased by 101 per RP capable of flow information definition.

1.1.7 *flow qos* (QoS Flow Information)

The QoS flow information is set. Items set by using this command include: the flow detecting condition parameters to detect input IP frames for which flow control is desired, priority decision on the detected flows, TOS rewriting, and flow control parameters to instruct the contract band surveillance. The maximum number of entries in the QoS list that can be prepared is 10,000 entries per device, a maximum of 2,000 entries for the filter list, and a maximum of 2,000 entries per P.R. However, the maximum number of entries that can be defined varies depending on the RM mounted memory size. Please refer to Table 1-35. Determination on the flow control is performed in the order of the list number specified in the input/output interface of the QoS flow information (the order of indication when the show flow qos is executed). Setting is not possible on the configuration definition qos-ip-list and the configuration definition filter-list.

Downloaded from www.Manualslib.com manuals search engine

Table 1-35 Maximum Definable Entries by Model and Each PM Mounting Memory Size

Model	RM Mounting Memory Size	Number of Entry (*1)		
		Unit	RP Unit	
			RP Type	--
GR2000-2S	All	1024 entries	RP-A1 or the equivalent	1024 entries (*2)
GR2000-4S	64MB, 128MB, 192MB	1024 entries	RP-D	1024 entries (*2)
			RP-D6,RP-DV	1024 entries
	256MB or more	2000 entries	RP-A1	1024 entries (*2)
			RP-D	2000 entries (*2)
			RP-D6,RP-DV	2000 entries
GR2000-6H	64MB, 128MB, 192MB	1024 entries	RP-A1, RP-C RP-D	1024 entries (*2)
			RP-C6, RP-D6, RP-CV, RP-DV	1024 entries
	256MB or more	6000 entries	RP-A1	1024 entries (*2)
			RP-C, RP-D	2000 entries (*2)
			RP-C6, RP-D6, RP-CV, RP-DV	2000 entries
GR2000-10H	64MB, 128MB, 192MB	1024 entries	RP-A1, RP-C RP-D	1024 entries (*2)
			RP-C6, RP-D6, RP-CV, RP-DV	1024 entries
	256MB or more	10000 entries	RP-A1	1024 entries (*2)
			RP-C, RP-D	2000 entries (*2)
			RP-C6, RP-D6, RP-CV, RP-DV	2000 entries
GR2000-20H	64MB, 128MB, 192MB	1024 entries	RP-A1, RP-C RP-D	1024 entries (*2)
			RP-C6, RP-D6, RP-CV, RP-DV	1024 entries
	256MB or more	10000 entries	RP-A1	1024 entries (*2)
			RP-C, RP-D	2000 entries (*2)
			RP-C6, RP-D6, RP-CV, RP-DV	2000 entries
GR2000-1B GR2000-2B GR2000-2B+	128MB	1024 entries	-	1024 entries
	256MB	2000 entries	-	2000 entries
GR2000-BH	512MB, 768MB, 1GB	2000 entries	-	2000 entries

**1: This indicates the total value of filter and QoS entries.*
**2: IPv6 QoS can not set on RP-A1, RP-C or RP-D.*

1.1.8 *flow qos* (IPv4)

Input Form

Setting and changing the global information by each input/output interface.

```
[set] flow qos <Interface Name> {in | out} [-disable]
```

Setting and changing the flow information.

```
[-action
[ {-upc <kbps> [-upc_burst <Byte>]}
| {[-max_rate <kbps> [-max_rate_burst <Byte>]]
```


Downloaded from www.Manualslib.com manuals search engine

```
        [-min_rate <kbps> [-min_rate_burst <Byte>]]} ]
    [-index <No.>]
    [-replace_exp <Value>]
    [-replace_user_priority <No.>]
    [ { [-priority <No.>][-discard <No.>]
    [{-penalty_drop | -penalty_discard <No.> | -group <No.>}] }
    | {  -replace_dscp <DSCP_Value>
    [{-penalty_drop | -penalty_dscp <DSCP_Value>}] }
    | {  -dscp_map [{-penalty_drop | -penalty_dscp <DSCP_Value>}] }] ]
```

[Normal packet flow detecting condition] and [Important packet flow detecting condition]

1. When all high order protocol is target.

   ```
   ip <IP_Source> <IP_Destination> [{dscp <DSCP_Value> | precedence
   <precedence_Value>}] [{upper| lower} <Length>] [exp <Value>]
   [user_priority <No.>]
   ```

2. When the high order protocol is other than TCP, UDP, ICMP and IGMP.

   ```
   <protocol No.> <IP_Source> <IP_Destination> [{dscp <DSCP_Value> |
   precedence <precedence_Value>}] [{upper| lower} <Length>] [user_priority
   <No.>]
   ```

3. When the high order protocol is TCP, UDP.

   ```
   {tcp| udp} <IP_Source> [<port_source>] <IP_Destination>
   [<port_destination>] [{dscp <DSCP_Value> | precedence
   <precedence_Value>}] [{upper| lower} <Length>] [user_priority <No.>]
   ```

4. When the high order protocol is ICMP.

   ```
   icmp <IP_Source> <IP_Destination> [<ICMP_Type> [<ICMP_Code>]] [{dscp
   <DSCP_Value> | precedence <precedence_Value>}] [{upper| lower} <Length>]
   [user_priority <No.>]
   ```

5. When the high order protocol is IGMP.

   ```
   igmp <IP_Source> <IP_Destination> [<IGMP_Type>] [{dscp <DSCP_Value> |
   precedence <precedence_Value>}] [{upper| lower} <Length>]
   [user_priority <No.>]
   ```

Note: 1: If the {normal packet flow detecting condition}, [premium {important packet flow detecting condition}], and the operation specification (*1) are set or changed simultaneously, input the operation specification after having input the {normal packet flow detecting condition}, and [premium {important packet flow detecting condition}].

2: When any parameter in the {normal packet flow detecting condition}, [premium {important packet flow detecting condition}] must be changed. Input all the flow detecting conditions and the operation specification again.

1: If the "flow detecting condition" and the operation designation

Downloaded from www.Manualslib.com manuals search engine

Changing only the operation designation.

```
[set] flow qos <Interface Name> {in | out} list <List No.> -action
     [ {-upc <kbps> [-upc_burst <Byte>]}
      | {[-max_rate <kbps> [-max_rate_burst <Byte>]]
      [-min_rate <kbps> [-min_rate_burst <Byte>]]} ]
     [-index <No.>]
     [-replace_exp <Value>]
     [-replace_user_priority <No.>]
[ { [-priority <No.>][-discard <No.>][{-penalty_drop | -penalty_discard
<No.> | -group <No.>}] }
| {  -replace_dscp <DSCP_Value> [{-penalty_drop | -penalty_dscp
<DSCP_Value>}] }
| {  -dscp_map [{-penalty_drop | -penalty_dscp <DSCP_Value>}] }] ]
```

Deletion of the information

```
delete flow qos <Interface Name> {in | out} [list <List No.>]
```

Indication of the information

```
show flow qos [<Interface Name> [{in | out} [list <List No.>]]]
```

Indication of a blank list number in the specified range

```
show flow qos <Interface Name> {in | out} [list <List No.>-<List No.>]
free
```

Indication of top blank list number in the specified range

```
show flow qos <Interface Name> {in | out} [list <List No.>-<List No.>]
free min_no
```

Parameters

The operation parameters are also decided with parameters that can be set according to the kinds of operations. The table below shows the parameters that can be set by operations.

Downloaded from www.Manualslib.com manuals search engine

Table 1-36 List of Parameters that Can Be Set for Each RP Type Using IPv4 QoS Information

Item		Parameter	RP-A1		RP-C, RP-D		RP-C6, RP-D6, RP-CV, RP-DV	
Main Item	Sub-Item		Input Side	Output Side	Input Side	Output Side	Input Side	Output Side
Flow detection conditions	Flow detection conditions	ip	√	√	√	√	√	√
	Protocol number	<protocol No.>	√	√	√	√	√	√
	Protocol TCP	tcp	√	√	√	√	√	√
	Protocol UDP	udp	√	√	√	√	√	√
	Protocol ICMP	icmp	√	√	√	√	√	√
	Protocol IGMP	igmp	√	√	√	√	√	√
	Source IP address	<IP_Source>	√	√	√	√	√	√
	Destination IP address	<IP_Destination>	√	√	√	√	√	√
	DSCP	dscp <DSCP_Value>	√	√	√	√	√	√
	precedence	precedence <precedence_Value>	√	√	√	√	√	√
Flow detection conditions (continued)	IP user data length	{upper | lower} <Length>	√	√	√	√	√	√
	Source port number	<Port_Source>	√	√	√	√	√	√
	Destination port number	<Port_Destination>	√	√	√	√	√	√
	ICMP type	<ICMP_Type>	√	√	√	√	√	√
	ICMP code	<ICMP_Code>	√	√	√	√	√	√
	IGMP type	<IGMP_Type>	√	√	√	√	√	√
	exp [ROUTE-OS7]	exp <EXP_Value>	--	--	√	--	√	--
	User priority	user_priority <No>	--	--	--	--	√	--
	Important packet	premium	--	--	√	√	√	--

Downloaded from www.Manualslib.com manuals search engine

Table 1-36 List of Parameters that Can Be Set for Each RP Type Using IPv4 QoS Information (continued)

Item		Parameter	RP-A1		RP-C, RP-D		RP-C6, RP-D6, RP-CV, RP-DV	
Main Item	Sub-Item		Input Side	Output Side	Input Side	Output Side	Input Side	Output Side
Designation of operation	Contract band	upc <kbps> upc_burst <Byte>	√ (*1)	√ (*1)	√	√	√	√
		min_rate <kbps> min_rate_burst <Byte>	--	--	√	√	√	√
		max_rate <kbps> max_rate_burst <Byte>	--	--	√	√	√	√
	Output priority	priority <No.>	√	√	√	√	√	√
	Queuing priority	discard <No.>	√	√	√	√	√	√
	DSCP rewrite	replace_dscp <DSCP_Value>	√ (*2)	√ (*2)	√ (*2)	√ (*2)	√ (*2)	√ (*2)
	Decision of priority by using DSCP of input IP packet.	dscp_map	√	√	√	√	√	√
	Abortion at contract band breach.	penalty_drop	√	√	√	√	√	√
	Queuing priority at contract band breach.	penalty_discard <No.>	√	√	√	√	√	√
	DSCP rewriting at contract band breach.	penalty_dscp <DSCP_Value>	√	√	√	√	√	√
	exp rewrite [ROUTE-OS7]	replace_exp <EXP_Value>	--	--	√	√	√	√
	Connection branch	index <No.>	--	--	--	√	--	√
	Group number	-group	--	--	--	--	--	√
	User priority rewrite	-replace_user_priority <No>	--	--	--	--	--	√

√: Can be set.
-: Cannot be set.
**1: Cannot be set for -upc_burst<Byte>*
**2: Can be set for unicast. Cannot be set for multi-cast..*
**3: RP-C cannot be set.*
**4: Only GR2000-1B, GR2000-2B and GR2000-2B+ can be set.*

The flow control type can be divided largely into 13 control types.

- Control 1:

  Determines the priority using the output priority.

- Control 2:

  Determines the priority using the output priority and performs surveillance on the contract band. If the detected flow breaches the contract band, abolishment processing is performed.

- Control 3:

  Determines the priority using the output priority and performs surveillance on the contract band. If the detected flow breaches the contract band, the priority is lowered.

- Control 4:

  Rewrites DSCP and uses it to determine the priority.

Downloaded from www.Manualslib.com manuals search engine

- Control 5:

  Rewrites DSCP, uses it to determine the priority and performs surveillance on the contract band. If the detected flow breaches the contract band, abolishment processing is performed.
- Control 6:

  Rewrites DSCP, uses it to determine the priority and performs surveillance on the contract band. If the detected flow breaches the contract band, the priority is lowered.
- Control 7:

  Determines the priority using the DSCP of the input IP packet.
- Control 8:

  Determines the priority using the DSCP of the input IP packet and performs surveillance on the contract band. If the detected flow breaches the contract band, abolishment processing is performed.
- Control 9:

  Determines the priority using the DSCP of the input IP packet and performs surveillance on the contract band. If the detected flow breaches the contract band, the priority is lowered.
- Control 10:

  Rewrites EXP and determines the priority.
- Control 11:

  Determines the priority using the EXP.
- Control 12:

  Makes allocation to groups.
- Control 13:

  Rewrites user priority.

Downloaded from www.Manualslib.com manuals search engine

Table 1-37 Operating Parameters that Can Be Set for Each Operation

Operation Parameter	Flow Control												
	1	2 (*1)	3 (*2)	4	5 (*1)	6 (*2)	7	8 (*1)	9 (*2)	10	11	12	13 (*6)
Existence of operating parameter -action	√	√	√	√	√	√	√	√	√	√	√	√	√
Contract band monitoring { -upc <kbps> [-upc_burst <Size>]| -min_rate <kbps> [-min_rate_burst <Byte>]| -max_rate <kbps> [-max_rate_burst <Byte>]| -max_rate <kbps> [-max_rate_burst <Byte>] -min_rate <kbps> [-min_rate_burst <Byte>]}		√	√		√	√		√	√				
Output priority -priority <No.>	x	x	√							x	x	x	x
Queuing priority -discard<No.>	x	x	x							x	x	x	x
User priority rewrite -replace_user_priority <No.>													√
Group number -group<No.>												√ (*5)	
DSCP rewrite -replace_dscp <DSCP_Value>				√	√	√							x
Priority designation by input IP packet DSCP -dscp_map							√	√	√				
Abortion at contract band breach. -penalty_drop		x (*3)			x(*3			x(*3)					
Queuing priority at contract band breach. -penalty_discard <No.>			√ (*4)										
DSCP rewriting at contract band breach. -penalty_dscp <DSCP_Value>						√ (*4)			√ (*4)				
EXP rewrite (mpls packet only) -replace_exp <Value>										√	√		
Output VC and DLCI designation -index <Value>	x	x	x	x	x	x	x	x	x	x	x	x	

√: Indispensable x: Can be set, and default. No mark: Setting is impossible.
**1: This is the operating parameter of contract band monitoring. These conditions cannot be set when "-min_rate<kbps>[-min_rate_burst<Byte>]" is specified. To guarantee the minimum band, this parameter can only change the queuing priority of a packet that violates the contract band.*
**2: This is the operating parameter of contract band monitoring. These conditions cannot be set when only "-max_rate<kbps> [-max_rate_burst<Byte>]" is specified. To limit the maximum band, this parameter can only discard a packet that violates the contract band.*
**3: This is the operating parameter of contract band monitoring. Omit these conditions when "-max_rate<kbps>[-max_rate_burst<Byte>]" is specified.*
**4: This is the operating parameter of contract band monitoring. The operation of a packet that violates the contract band of "-min_rate<kbps>" is specified when "-max_rate<kbps>[-max_rate_burst<Byte>] -min_rate<kbps>[min_rate_burst<Byte>]" is specified.*
**5: No setting is possible on the VLAN line.*
**6: Only VLAN lines can be set. In addition, output priority determination and DSCP rewrite cannot be set simultaneously.*

Downloaded from www.Manualslib.com manuals search engine

Parameter

`<Interface name>`

Description: Specifies the subject interface name set in the ip information or ip-address information. (The ip information or the ip-address information should be set before inputting this command.) RM Ethenet and Tunnel interface are not supported. For details, refer to Table 1-5.

Default: No default is possible.

`{ in | out}`

Description: Specifies the Inbound/Outbound. Either one or both of the Inbound/Outbound can be set against one interface.

in: Inbound (specification of the frame input side)

out: Outbound (specification of the frame output side)

Default: No default is possible.

`[-disable]`

Description: Nullifies the flow control by input/output interface.

Default: Flow control is executed.

`list <List No.>`

Description: Specifies the list number.

Default: Default is possible only in the indicated case. All the lists are displayed at default.

Range of value: 1 to 20,000 (ten-decimals)

`[list <List No.>-list <list No.>]`

Description: Specifies the range of a list number. This parameter can be specified only when a blank list number is displayed.

Default: The range of the list number being the object of indication will the number of all the lists totaling the IPv4QoS list and IPv6QoS list.

Range of value: 1-255 (decimal) are designated to <No>. (Ver. 05-01, Ver. 06-00)
1-1000000 (decimal) are designated to <No.>. (Ver. 06-01)

`free`

Description: Displays the blank list number.

Default: Cannot be omitted when the blank list number is displayed.

`min_no`

Description: Displays the top blank list number in the specified range.

Default: Cannot be omitted when the top list number of a blank list number is displayed.

Downloaded from www.Manualslib.com manuals search engine

- Flow detecting condition parameter:

```
{ ip | <protocol No.> | tcp | udp | icmp | igmp }
```

Description: Specifies the high-order protocol number of the protocol name. If all the protocols are taken as the object, ip is specified.

Default: No default is possible.

Range of value: 0 to 255 (ten-decimals). (Please refer to Table 1-20.)

Table 1-38 General protocol number

Protocol No.	Protocol
1	ICMP
6	TCP
8	EGP
17	UDP
88	IGRP
89	OSPF

```
<ip_source>
```

Specifies the transmitter IP address.

If address to be designated is one:nnn.nnn.nnn.nnn

If address is designated by range:nnn.nnn.nnn.nnn-nnn.nnn.nnn.nnn

If designated by sub-net mask length:nnn.nnn.nnn.nnn/aa

If all IPv4 addresses are designated:any

Default: No default is possible.

Range of value: IP address (nnn, nnn, nnn, nnn): 0.0.0.0-255.255.255.255
Sub-net mask length (aa): 0-32

```
<ip_destination>
```

Specifies the destination IP address.

If address to be specified is one:nnnn:nnnn:nnnn:nnnn:nnnn

If address is specified by range: nnn.nnn.nnn.nnn-nnn.nnn.nnn.nnn

If designated by sub-net mask length:nnn.nnn.nnn.nnn/aa

If all the IP addresses are specified:any

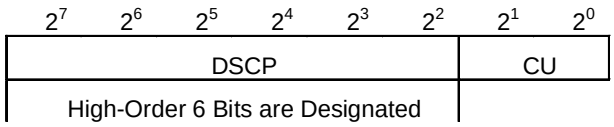
Default: No default is possible.

Range of value: IP address (nnnn:nnnn:nnnn:nnnn):
0:0:0:0:0:0:0:0-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Sub-net mask length (aaa)0-32

```
[dscp <DSCP_Value>][Ver.06-01]
```

This parameter enables the function that rewrites a DSCP value. It rewrites the DSCP value that is the upper six bits of a TOS field. The lower two bits of a TOS field are not rewritten.



DSCP (Differentiated Services Code Point), CU (Current Unused)

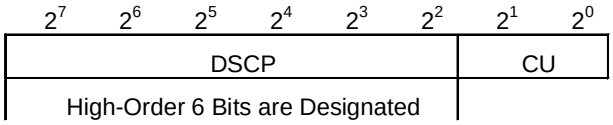
Downloaded from www.Manualslib.com manuals search engine

Default: None (DSCP values are not included in the flow detecting condition.)

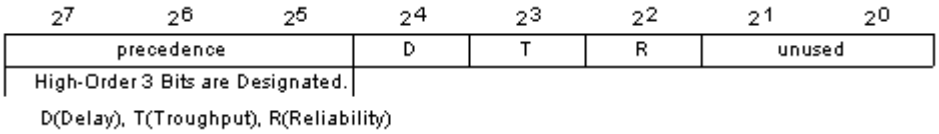
Range of value: 0 to 63 (decimal).

`[precedence <precedence_Value>]`

This parameter specifies precedence value, which is the upper 3 bits of the ToS field. This is compared to the upper 3 bits of the ToS field of sent/received packets. The lower 5 bits of the ToS field are ignored.



DSCP (Differentiated Services Code Point), CU (Current Unused)



Default: None (precedence values are not included in the detecting condition)

Range of value: 0 - 7 (decimal)

`[{ upper | lower } <Length>`

Specifies the upper or lower limit of the IP user data length.

-upper:Upper limit of the IP user data length is designated.

-lower:Lower limit of the IP user data length is designated.

Default: None (TOS values are not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal).

Table 1-39 Relationship Between Upper and Lower IP User Data Length Limits and IP User Data Length

Upper and Lower Limits Designation	Relationship between A (packet value) : (Total Length) - (Header Length)) and B (IP user data length designated in constituting definition information)	Result
-upper	A ≤ B	Agreed.
-upper	A > B	Disagreed.
-lower	A ≥ B	Agreed.
-lower	A < B	Disagreed.

Downloaded from www.Manualslib.com manuals search engine

-exp <Value>[ROUTE-OS7]

Description: Specifies the value of the EXP field. Setting is possible only in the ordinary packet flow detecting condition. The list information set by this parameter should be specified as the flow control of the input side that specified in (Inbound). If specified out (Outbound), the specification is invalid. In addition, the conditions of the said parameter are invalid even if other flow detecting condition parameters are set. The number of packets that coincide with the flow detection conditions is not displayed. (This parameter is valid for RP-CV and RP-DV.)

Default: None.

Range of value: 0 to 7.

[<port_source>]

Specifies the transmitter port number.

If port to be specified is one: nnnnn

If port number is specified by range:nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-25.)

[<port_destination>]

Specifies the destination port number.

If port to be specified is one: nnnnn

If port number is specified by range:nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-25.)

Table 1-40 General ICMP Type Code Number

Port Dumber (Decimal)	Name
20/tcp	File Transfer [Default Data]
21/tcp	File Transfer [Control]
22/tcp	Secure Shell Login
23/tcp	Telnet
25/tcp	Simple Mail Transfer
53/tcp 53/udp	Domain Name Server
80/tcp	World Wide Web HTTP
110/tcp 10/udp	Post Office Protocol - Version 3
161/udp	SNMP

[<ICMP_Type>]

Description: Specifies the IGMP type.

Default: None. (The IGMP type is not included in the flow detecting condition.)

Downloaded from www.Manualslib.com manuals search engine

Range of value: 0 to 255 (ten-decimals). (Please refer to Table 1-41.)

[<ICMP_Code>]

Description: Specifies the IGMP type.

Default: None. (The IGMP type is not included in the flow detecting condition.)

Range of value: 0 to 255 (ten-decimals). (Please refer to Table 1-41.)

Table 1-41 Genral IGMP Type Code Number

Type	Name	Code
0	Echo Reply	0
3	Destination Unreachable	0-12
4	Source Quench	0
5	Redirect	0-3
8	Echo	0
11	Time Exceeded	0-1
12	Parameter Problem	0
13	Timestamp	0
14	Timestamp Reply	0
17	Address Mask Request	0
18	Address Mask Reply	0

[<IGMP_Type>]

Description: Specifies the IGMP type.

Default: None. (The IGMP type is not included in the flow detecting condition.)

Range of value: 0 to 255 (ten-decimals). (Please refer to Table 1-42.)

Table 1-42 General ICMP type number

Type	Name
17	Membership Query
18	Version 1 Membership Report
19	DVMRP protocol
22	Version 2 Membership Report
23	Version 2 Leave Group
34	Version 3 Membership Report

[user_priority <No.>]

Description: Specifies user priority. This parameter specify "in"(Inbound) VLAN line information.

Default: None

Range of value: 0 -7

Downloaded from www.Manualslib.com manuals search engine

Ordinary packet flow detecting condition} [premium {important packet flow detecting condition}]

When the maximum band restriction (-max_rate) or the minimum band assurance (-min_rate) is executed, the important packet is transferred with priority given in the band, and the ordinary packet is transferred when the important packet is not transferred by using all the bands. This function is called the important packet assuring function.

The flow detecting conditions for the ordinary packet are inputted before the premium, and the flow detecting conditions for the important packet after the premium. The flow detecting conditions for the important packet can be set only after either one of the maximum band restriction

(-max_rate) or the minimum band assurance (-min_rate) has been set.

The parameters that have not been set in the important packet flow detecting conditions are subjected to the same conditions as the parameters that have been set in the ordinary packet flow detecting conditions. For setting the important packet flow detecting conditions, set only the flow detecting condition parameters whose detecting conditions differ from the ordinary packet flow detecting conditions.

When the important packet protecting function is used, the number of entries used per list becomes two or four entries. (*1)

(This parameter is effective only for RP-C and RP-D.)

Default: None. (The important packet protecting function is not used.)

Range of value: [<ICMPv6_Code>]

- Operation parameter

`[-action]`

If the operation parameter is either set or changed, please be sure to set this parameter at the head of the whole operation parameter.

Default: None (No default is possible when designating the operation.)

Range of value: None

`[-upc <kbps> [-upc_burst <Byte>]]`

Specifies the contract band by kbit/s. Specifies burst size in byte unit. If a value greater than the line speed is set, no action at breach is taken.

When setting this parameter, it is not possible to set -max_rate, -max_burst, and min_rate_rate, -min_rate_burst. (-upc_burst is effective only in RP-C, RP-D, RP-D6, RP-CV, RP-DV, GR2000-1B, GR2000-2B, GR2000-2B+ and GR2000-BH.)

Default: None. (No contract band surveillance is executed.)

Range of value: <kbps>: 0 to 2400000 (0 to 2.4G) (10-decimals).

If 0 to 11 is specified in the case of RP-A, the operation is performed by taking the contract band as 12[kbps].

If 0 to 4 is specified in the case of RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B, GR2000-2B, GR2000-2B+ and GR2000-BH, the operation is performed by taking the contract band as 4.1[kbps].

<Byte>: 0 to 131072 (10-decimals)

Downloaded from www.Manualslib.com manuals search engine

[-max_rate <kbps> [-max_rate_burst <Byte>]]

Specifies the maximum contract band restriction by kbit/s. Specifies burst size in byte unit. If a value greater than the line speed is set, no action at breach is taken.

When setting this parameter, it is not possible to set -upc, or -upc_burst.

Packets exceeding the maximum band when setting this parameter are all discarded.

When this is used, the number of entries used per list may become two or four entries.

(This parameter is effective only for RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B and GR2000-2B.)

Default: None. (No contract band surveillance is executed.)

Range of value: <kbps>: 0 to 2400000 (0 to 2.4G) (10-decimals).

If 0 to 11 is specified in the case of RP-A, the operation is performed by taking the contract band as 12[kbps].

If 0 to 4 is specified in the case of RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B, GR2000-2B, GR2000-2B+ and GR2000-BH, the operation is performed by taking the contract band as 4.1[kbit/s].

<Byte>: 0 to 131072 (10-decimals)

[-min_rate <kbps> [-min_rate_burst <Byte>]]

Specifies the minimum band assurance by kbit/s. Specifies burst size in byte unit. If a value greater than the line speed is set, no action at breach is taken.

When setting this parameter, it is not possible to set -upc, or -upc_burst.

When this parameter is used, the number of entries used per list may become two or four entries. (*1)

(This parameter is effective only for RP-C and RP-D.)

Default: None. (No contract band surveillance is executed.)

Range of value: <kbps>: 0 to 2400000 (0 to 2.4G) (10-decimals).

If 0 to 11 is specified in the case of RP-A, the operation is performed by taking the contract band as 12[kbit/s].

If 0 to 4 is specified in the case of RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B, GR2000-2B, GR2000-2B+ and GR2000-BH, the operation is performed by taking the contract band as 4.1[kbit/s].

<Byte>: 0 to 131072 (10-decimals)

[-index <No.>]

Specifies the connection branching index number (index specified in the DLCI group information or the Ve-Group information). It selects and transmits DLCI/VC specified in the group when relaying the packet that agrees with the flow detecting conditions. For the list information setting the connection branching index number, specify out (Outbound) as the flow control of the output side.

(This parameter is effective only for RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B, GR2000-2B and GR2000-2B+.)

Default: None.

Downloaded from www.Manualslib.com manuals search engine

Range of value: 0 to 7.

`[-priority <No.>] [-discard <No.>]`

Makes the flow control function effective by specifying the output priority and queuing priority. Sets the priority in <No.>. The priority parameter is used as the output priority in the case of output priority control and as the queue number in the case of minimum band assurance. If the output line is an ATM line, it sets the value of the cell loss priority indication (CLP bit) of the cells transmitting in VC using either the "output" priority or the "queuing" priority. To set the cell loss indication bit, refer to the parameters defined in the *GR2000 Configuration Commands, (universal CLI) Vol. 1*, vc (VC information)." If the VC's service category is GRR or GFR2, select the "queuing" priority from the VC priority queue. If the VC's service category is GFR2, set the output priority from the VC priority queue. For the queuing and output priority of VC priority queuing, refer to the *GR2000 Applications Guide*.

When setting this parameter, it is not possible to -replace_dscp or -dscp_map.

Default: priority: 4
discard: 4

Range of value: -priority <No.>: 1 to 1000
(In case of the output priority control, the greater the value of the output priority, the more preferentially the packet is issued.)

-discard <No.>: 1 to 4.
(The smaller the value of the queuing priority, the more preferentially the packet is discarded.)

The ranges for the output priority (priority) and the queuing priority (discard) vary depending on the setting conditions.

Table 1-43 Relationship Between Number of Queues and Priority

Setting Condition		Range	
Interface Using this List	**No. of Queue in Output Interface**	**Output Priority (*1)**	**Queuing Priority**
Input side	--	1-8	1-4
Output side	4	1-4	1-4
Output side	8	1-8	1-4
Output side	16	1-16	1-4
Output side	32	1-32	1-4
Output side	64	1-64	1-4
Output side	250	1-250	1-4 (*2)
Output side	1000	1-1000	1-4 (*2)

**1: If value outside the range is set in output priority, the setting contents are nullified.*
**2: If the QoS attribute of the output interface is the minimum band assurance (specified by kbps), the flow control is executed as follows:*

- *Queuing priority 1 and 2: Flow control is executed at queuing priority 2.*
- *Queuing priority 3 and 4: Flow control is executed at queuing priority 4.*

`[-group <No.>] [ROUTE-OS6B]`

Designates the group number to be outputted when the output line transmission control is the group band control relative to the Line. Setting is possible only

Downloaded from www.Manualslib.com manuals search engine

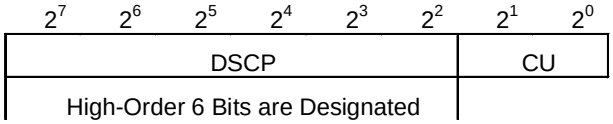
when the group number has been previously set in the QoS interface information. Designate this parameter's out (Outbound) as the flow control of the output side. When this parameter is designated, only "-priority" and "-discard" can be set. The setting range for "-priority" is from one to four. This parameter cannot be set if the output line is a VLAN line.

Default: None

Range of value: The group number designated by the qos-interface (QoS interface information).

`[-replace_dscp <DSCP_Value>]`

This parameter enables the function that rewrites a DSCP value and that determines the output priority and queuing priority using the rewritten DSCP value. The DSCP value and its corresponding output priority and queuing priority are specified using a qos-tos-map command. This parameter rewrites the DSCP value that is the upper six bits of a TOS field. The lower two bits of a TOS field are not rewritten.



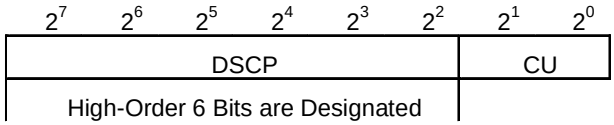
DSCP (Differentiated Services Code Point), CU (Current Unused)

Default: priority: 4
discard: 4

Range of value: -replace_dscp <DSCP_Value>: 0 to 63 (decimal).

`[-dscp_map]`

This parameter enables the function that determines the output priority and queuing priority using the DSCP value of an input packet. The DSCP value and its corresponding output priority and queuing priority are specified using a qos-tos-map command. The upper six bits of a TOS field in a receive packet are treated as a target. The lower two bits of a TOS field are ignored. -priority, -discard, and -replace_dscp cannot be set when this parameter is set.



DSCP (Differentiated Services Code Point), CU (Current Unused)

Default: priority: 4
discard: 4

`[{-penalty_drop | -penalty_discard <No.> | -penalty_dscp <DSCP_Value>}]`

Specifies the operation when the contract band is breached.

`-penalty_drop`: Packet discard.

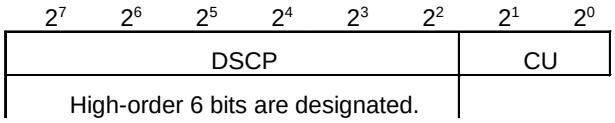
`-penalty_discard <No.>`:
Specifies the queuing priority after having been changed. If this parameter is specified and the out put line is ATM, it is possible to set the cell loss priority indication bit (CLP bit) of a

Downloaded from www.Manualslib.com manuals search engine

cell transmitted by VC to zero when the queuing priority is three or four, and to one when the queuing priority is one or two. For setting the cell loss indication bit, please refer to in *GR2000 Configuration Commands, (universal CLI) Vol. 1*.

`-penalty_dscp <DSCP_Value>`

This parameter enables the function that specifies a DSCP rewrite value and that determines the output priority and queuing priority using the rewritten DSCP value. The DSCP value and its corresponding output priority and queuing priority are specified using a qos-tos-map command. However, the upper six bits of a TOS field are rewritten and the lower two bits are ignored. [Ver. 06-01]



DSCP(Differentiated Services Code Point), CU(Current Unused)

Default: -upc setting: -penalty_drop
-max_rate setting: -penalty_drop (All packets that violate the -maximum band are discarded.)
-min_rate setting: -discard 1 (A packet that violates the minimum band is made easy to discard.)

Range of value: -penalty_dscp<DSCP_Value>: 0 to 63 (Decimal)
-penalty_discard<No.>: 1 to 4
(The queuing priority value is preferentially discarded as it decreases.)

The range of queuing priority (-penalty_discard) during contract band violation varies depending on the setting conditions.

Table 1-44 Relationship Between Number of Queues and Priority

Setting Condition		Range
Interface Using this List	**No. of Queue in Output Interface**	**Queuing Priority**
Input side	--	1-4
Output side	4	1-4
Output side	8	1-4
Output side	16	1-4
Output side	32	1-4
Output side	64	1-4
Output side	250	1-4 (*2)
Output side	1000	1-4 (*2)

**1: If value outside the range is set in output priority, the setting contents are nullified.*
**2: If the QoS attribute of the output interface is the minimum band assurance (specified by kbit/s), the flow control is executed as follows:*
- *Queuing priority 1 and 2: Flow control is executed at queuing priority 2.*
- *Queuing priority 3 and 4: Flow control is executed at queuing priority 4.*

Downloaded from www.Manualslib.com manuals search engine

[-replace_exp <Vlue>[ROUTE-OS7]]

Specifies the rewriting value for the EXP field.

(This parameter is valid for RP-CV and RP-DV.)

Default: None.

Range of value: 0 to 7.

-replace_user_priority <No.>

Specifies the rewriting value for user priority.

Use this parameter to specify "out" (outbound) VLAN line information as flow control on the outbound side. When this parameter is set, it is only possible to set -priority, -discard and -replace dscp.

Default: None

Range of value: 0 - 7

The number of entries used per list as a result of setting the important packet protecting function, maximum band restriction, and minimum band assurance is as shown in Table 1-45.

Table 1-45 Number of Entries Used per List by Each Setting

Setting Contents	Setting Parameter			Number of Entry
	-premium	*-max_rate*	*-min_rate*	
No setting				1
Maximum band restriction		√		1
Minimum band assurance			√	1
Maximum band restriction + minimum band assurance		√	√	2
Maximum band restriction + important packet protection	√	√		2
Minimum band assurance + important packet protection	√			2
Maximum band restriction +minimum band assurance + important packet protection	√	√	√	4
√: With setting. No mark : Without setting				

Input Examples

1. Setting the IPv4 QoS flow information
   - Classification of packets:
     In order to preferentially transfer the packets with the transmitter IP addresses of 10, 10, 10, 2, the high-order protocol of TCP, and with the destination port number of 23 (telnet), the output priority class of the said packets are specified as seven and that of other packets as one.

```
(config)#  flow qos Tokyo out list 1 tcp 10.10.10.2 any 23 action priority
7
(config)#  flow qos Tokyo out list 2000 ip any any action priority 1
(config)#  flow -yes
(config)#  show flow
flow yes {
        qos Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action priority 7;
                list 2000 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Contract band specification:
  Specifies to monitor traffics from end users by using ISP and discard the packets breaching the contract band. Specifies that packets with the interface name of Tokyo and the transmitter address of 10.10.10.0/24 to be monitored in the contract band of 128 kbit/s.

```
(config)#  flow qos Tokyo in list 1 ip 10.10.10.2 any action upc 128
(config)#  flow yes
(config)#  show flow
flow yes {
        qos Tokyo in {
                list 1 ip 10.10.10.2 any action upc 128;
        };
};
(config)#
```

- Specification of queuing priority when contract band is breached:
  Specifies that packets breaching the contract band be discarded more easily when the output lines are congested. Monitors the packets with the interface name of Tokyo and the transmitter address of 10.10.10.0/24 in the contract band of 5,000 kbit/s and changes the queuing priority to one at breach.

```
(config)#  flow qos Tokyo in list 1 ip 10.10.10.0/24 any -action -upc 5000
penalty_di
scard 1
(config)#  flow -yes
(config)#  show flow
flow yes {
        qos Tokyo in {
              list 1 ip 10.10.10.0/24 any action upc 5000 penalty_discard
1;
        };
};
(config)#
```

- Specifying the maximum band restriction + minimum band assurance:
  Sets the maximum band restriction and the minimum band assurance by each end user by using ISP. Specifies the users with the interface name of Tokyo and the transmitter addresses of 10.10.10.1 and 10.10.10.2 with the maximum band restriction band of 128 kbit/s and the minimum band assurance band of 64 kbit/s.

```
(config)#  flow qos Tokyo out list 1 ip any 10.10.10.1 -action -max_rate
128 -min_ra
te 64
(config)#  flow qos Tokyo out list 2 ip any 10.10.10.2 -action -max_rate
128 -min_ra
te 64
(config)#  flow -yes
(config)#  show flow
flow yes {
        qos Tokyo out {
                list 1 ip any 10.10.10.1 action max_rate 128 min_rate 64;
                list 2 ip any 10.10.10.2 action max_rate 128 min_rate 64;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Specifying the maximum band restriction + minimum band assurance + important packet protecting function:
  Sets the maximum band restriction, the minimum band assurance, and important packet protecting function for each end user by using ISP. Specifies that the users with the interface name of Tokyo and the transmitter address of 10.10.10.1 have a maximum band restriction band of 128 kbit/s and the minimum band assurance band of 64 kbit/s, gives the important packet a DSCP value of 20, and the other packets TOS values different from that.

```
(config)#  flow qos Tokyo out list 1 ip any 10.10.10.1 premium ip any any
dscp 20 -action -max_rate 128 -min_rate 64
(config)#  flow yes
(config)#  show flow
flow yes {
        qos Tokyo out {
               list 1 ip any 10.10.10.1 premium ip any any dscp 20 action
max_rate 128 min_rate 64;
        };
};
(config)#
```

- Connects two bases by two VCs, and allots them to separate VCs according to flow:
  Allots the VC with the connection branching index number one to packets whose transmitter IP addresses are 10.10.10.2 to 10.10.10.5, and the VC with the connection branching index number zero to packets with the transmitter addresses other than those above.

```
(config)#  flow qos Tokyo out list 1 ip 10.10.10.2-10.10.10.5 any -action
-index 1
(config)#  flow qos Tokyo out list 2 ip any any -action -index 0
(config)#  flow -yes
(config)#  show flow
flow yes {
        qos Tokyo out {
                list 1 ip 10.10.10.2-10.10.10.5 any action index 1;
                list 2 ip any any action index 1;
        };
};
(config)#
```

- DSCP value rewriting:
  Rewrites the DSCP value according to each traffic flow received from end users. Rewrites the DSCP value of the packets with the transmitter IP address of 10.10.10.1 to 34 and those with 10.10.10.2 to 20.

```
(config)#  flow qos Tokyo in list 1 ip 10.10.10.1 any action -replace_dscp
34
(config)#  flow qos Tokyo in list 2 ip 10.10.10.2 any action -replace_dscp
20
(config)#  flow -yes
(config)#  show flow
flow yes {
        qos Tokyo in {
                list 1 ip 10.10.10.1 any action replace_dscp 34;
                list 2 ip 10.10.10.2 any action replace_dscp 20;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Setting the precedence comparison function:
  The following is a setting example with user priority set to 1 when the send packet precedence value is 7.

```
(config)# flow -yes -precedence_mask
(config)# flow qos Tokyo1 out list 1 ip any any precedence 7 -action
-replace_user_priority  1
(config)# show flow
flow yes {
        precedence_mask;
        qos Tokyo1 out {
              list 1 ip any any precedence 7 action replace_user_priority
1;
        };
};
```

2. Inserting the list
   The list number three is inserted between the list numbers one and five.

```
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action priority 7;
                list 5 ip any any action priority 1;
        };
};
(config)#  flow qos Tokyo out list 3 tcp any any -action -priority 4
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action priority 7;
                list 3 tcp any any action priority 4;
                list 5 ip any any action priority 1;
        };
};
(config)#
```

3. Nullification of QoS flow information by each input/output interface
   Nullifies the QoS flow control of the output interface Tokyo.

```
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action priority 7;
                list 5 ip any any action priority 1;
        };
};
(config)#  flow qos Tokyo out -disable
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out disable {
                list 1 tcp 10.10.10.2 any 23 action priority 7;
                list 5 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Changing the parameter

   - Changing the parameters for flow detecting conditions and operation specification
     Changes the parameters for flow detecting conditions and operation specification in the list of the list number one.

```
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 tcp 10.10.10.2 any 23 action priority 7;
                list 5 ip any any action priority 1;
        };
};
(config)#  flow qos Tokyo out list 1 udp 20.20.20.20 any -action -priority
6
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 udp 20.20.20.20 any action priority 6;
                list 5 ip any any action priority 1;
        };
};
(config)#
```

   - Changing only the parameter for operation specification
     Changes the parameters in the list of the list number one from the output priority of six to the output priority of two.

```
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 udp 20.20.20.20 any action priority 6;
                list 5 ip any any action priority 1;
        };
};
(config)#  flow qos Tokyo out list 1 -action -priority 2
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 udp 20.20.20.20 any action priority 2;
                list 5 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

5. Deleting the QoS flow information

- Deleting the input/output interface unit
  Deletes the QoS flow information of the input/output interface Tokyo.

```
(config)#  show flow qos
flow yes {
        qos Tokyo in {
                list 1 ip 10.10.10.2 any action replace_dscp 40;
        };
        qos Tokyo out {
                list 1 ip any 10.10.10.1 action priority 2;
                list 5 ip any any action priority 1;
        };
};
(config)#  delete flow qos Tokyo out
(config)#  show flow qos
flow yes {
        qos Tokyo in {
                list 1 ip 10.10.10.2 any action replace_dscp 40;
        };
};
(config)#
```

- Deleting the list unit
  Deletes the list number one of the output interface Tokyo.

```
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 ip any 10.10.10.1 action priority 2;
                list 5 ip any any action priority 1;
        };
};
(config)#  delete flow qos Tokyo out list 1
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 5 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Deleting the parameters for operation specification
  Deletes the operation specification in the list number one of the output interface Tokyo.

```
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 ip any 10.10.10.1 action priority 2;
                list 5 ip any any action priority 1;
        };
};
(config)#  delete flow qos Tokyo out list 1 -action
(config)#  show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 1 ip any 10.10.10.1;
                list 5 ip any any action priority 1;
        };
};
(config)#
```

6. Displaying the QoS flow information
   - Displaying all the input/output interface
     Displays the QoS flow information for the entire input/output interface.

```
(config)#  show flow qos
flow yes {
        qos Tokyo in {
                list 1 ip 10.10.10.2 any action replace_dscp 40;
        };
        qos Osaka out {
                list 1 ip any 10.10.10.1 action priority 2;
                list 5 ip any any action priority 1;
        };
};
(config)#
```

   - Displaying the input/output interface unit
     Displays the QoS flow information for the input/output interface Osaka.

```
(config)#  show flow qos Osaka out
flow yes {
        qos Osaka out {
                list 1 ip any 10.10.10.1 action priority 2;
                list 5 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Displaying the list unit
  Displays the QoS flow information of the list number five for the input/output interface Osaka.

```
(config)#  show flow qos Osaka out list 5
flow yes {
        qos Osaka out {
                list 5 ip any any action priority 1;
        };
};
(config)#
```

7. Display of blank list number
   - Display of all blank list numbers
     Display all blank list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in free
Free number: 5,7,15-20000
(config)#
```

   - Display of blank list number in the specified range
     Display all blank list numbers in the range in which the list number is 1 to 100 on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in list 1-100 free
Free number: 5,7,15-100
(config)#
```

   - Display of top blank list number in all list numbers
     Display the top blank list number in the list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in free min_no
Free number: 5
(config)#
```

   - Display of top blank list number in the specified range
     Display the top blank list number in the range in which the list number is 51 to 100 on the Inbound (input) side of interface Tokyo.

```
(config)#  show flow qos Tokyo in list 51-100 free min_no
Free number: 51
(config)#
```

Related Commands

flow, flow filter, qos, qos-tos-map, qos-ip-list, filter-list, nat, nat inside interface, nat outside interface

Downloaded from www.Manualslib.com manuals search engine

Related Information

For the flow control, please refer to the *GR2000 Applications Guide*.

Precautions

1. Determination of the QoS flow is performed in the order of the list number specified in the input/output interface in the QoS flow information (the order of display when show flow qos is executed).
2. When setting the qos-ip-list (QoS IP frame condition information) or filter-list (filter list information), this command cannot be set. Delete both the qos-ip-list and filter-list before setting this command.
3. Rewriting the EXP in the MPLS net has the following restrictions.

   The list is effective if the EXP rewriting is set in the output side list. However, if set in the input side list, the action is not guaranteed. Always set the EXP rewriting on the output side list.
4. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
5. Flow information consumes 101 entries in each RP when address conversion (nat) is set. Therefore, when address conversion (nat) is set, the maximum entry count is decreased by 101 per RP capable of flow information definition.

1.1.9 *flow qos* (IPv6) [ROUTE-OS6]

Input Format

Setting

- Setting and changing the global information by each input/output interface.

```
[set] flow qos <Interface Name> {in | out} [-disable]
```

- Setting and changing the flow information.

```
[set] flow qos <Interface Name> {in | out} [-disable] list <List No.>
[-action
[ {-upc <kbps> [-upc_burst <Byte>]}
| {[-max_rate <kbps> [-max_rate_burst <Byte>]]
[-min_rate <kbps> [-min_rate_burst <Byte>]]} ]
[-index <No.>]
[-replace_user_priority <No.>]
[ { [-priority <No.>][-discard <No.>][{-penalty_drop | -penalty_discard
<No.>|-group<No.>}] }
| {  -replace_dscp <DSCP_Value> [{-penalty_drop | -penalty_dscp
<DSCP_Value>}] }
| {  -dscp_map [{-penalty_drop | -penalty_dscp <DSCP_Value>}] }] ]
```

[Normal packet flow detecting condition] and [Important packet flow detecting condition]

1. When the high order protocol is other than TCP, UDP, and IGMPv6.

```
{ip | <protocol No.>} <IPv6_Source> <IPv6_Destination> [{dscp
```


Downloaded from www.Manualslib.com manuals search engine

```
<DSCP_Value> | precedence <precedence_Value>}] [{upper| lower} <Length>]
[user_priority <No.>]
```

2. When the high order protocol is TCP, UDP.

```
{tcp| udp} <IPv6_Source> [<port_source>] <IPv6_Destination>
[<port_destination>] [{dscp <DSCP_Value> | precedence
<precedence_Value>}] [{upper| lower} <Length>] [user_priority <No.>]
```

3. When the high order protocol is ICMPv6.

```
icmp6 <IP_Source> <IP_Destination> [<ICMPv6_Type> [<ICMPv6_Code>]] [{dscp
<DSCP_Value> | precedence <precedence_Value>}] [{upper| lower} <Length>]
[user_priority <No.>]
```

Note: 1: If the {normal packet flow detecting condition}, [premium {important packet flow detecting condition}], and the operation specification (*1) are set or changed simultaneously, input the operation specification after having input the {normal packet flow detecting condition}, and [premium {important packet flow detecting condition}].

2: When any parameter in the {normal packet flow detecting condition}, [premium {important packet flow detecting condition}] must be changed. Input all the flow detecting conditions and the operation specification again.

1: If the "flow detecting condition" and the operation designation

Changing only the operation designation:

```
[set] flow qos <Interface Name> {in | out} list <List No.> -action
[ {-upc <kbps> [-upc_burst <Byte>]}
| {[-max_rate <kbps> [-max_rate_burst <Byte>]]
[-min_rate <kbps> [-min_rate_burst <Byte>]]} ]
[-index <No.>]
[-replace_user_priority <No.>]
[ { [-priority <No.>][-discard <No.>][{-penalty_drop | -penalty_discard
<No.> | -group <No.>}] }
| {  -replace_dscp <DSCP_Value> [{-penalty_drop | -penalty_dscp
<DSCP_Value>}] }
| {  -dscp_map [{-penalty_drop | -penalty_dscp <DSCP_Value>}] }]
```

Deletion of the information

```
delete flow qos <Interface Name> {in | out} [list <List No.>]
```

Indication of the information

```
show flow qos [<Interface Name> [{in | out} [list <List No.>]]]
```

Indication of a blank list number in the specified range

```
show flow qos <Interface Name> {in | out} [list <List No.>-<List No.>]
free
```

Indication of top blank list number in the specified range

```
show flow qos <Interface Name> {in | out} [list <List No.>-<List No.>]
free min_no
```


Downloaded from www.Manualslib.com manuals search engine

Parameter

Parameters that can be set for each RP type have been determined. IPv6 QoS can be executed using RP-C6, RP-D6,GR2000-1B, GR2000-2B, GR2000-2B+ and GR2000-BH but cannot be executed using RP-A1, RP-C, and RP-D. The list of parameters that can be set for each RP type using IPv6 QoS information is shown in Table 1-46 List of Parameters that Can Be Set for Each RP Type Using IPv6 QoS Information.

Table 1-46 List of Parameters that Can Be Set for Each RP Type Using IPv6 QoS Information.

Item		Parameter	RP-A1		RP-C, RP-D		RP-C6, RP-D6, RP-CV, RP-DV GR2000-1B/2B	
Main Item	Sub-Item		Input Side	Output Side	Input Side	Output Side	Input Side	Output Side
Flow detection conditions	All protocol IPs	ip	–	–	–	–	√	√
	Protocol number	<protocol No.>	–	–	–	–	√	√
	Protocol TCP	tcp	–	–	–	–	√	√
	Protocol UDP	udp	–	–	–	–	√	√
	Protocol ICMP6	icmp6	–	–	–	–	√	√
	Source IP address	<IP_Source>	–	–	–	–	√	√
	Destination IP address	<IP_Destination>	–	–	–	–	√	√
	DSCP	dscp <DSCP_Value>	–	–	–	–	√	√
	precedence	precedence <precedence_Value>	–	–	–	–	√	√
	IP user data length	{upper | lower} <Length>	–	–	–	–	√	√
	Source port number	<Port_Source>	–	–	–	–	√	√
	Destination port number	<Port_Destination>	–	–	–	–	√	√
	ICMPv6 type	<ICMPv6_Type>	–	–	–	–	√	√
	ICMPv6 code	<ICMPv6_Code>	–	–	–	–	√	√
	User priority	user_priority <No.>	–	–	–	–	√	–
	Important packet	premium	–	–	–	–	√	√

Downloaded from www.Manualslib.com manuals search engine

Table 1-46 List of Parameters that Can Be Set for Each RP Type Using IPv6 QoS Information.

Item		Parameter	RP-A1		RP-C, RP-D		RP-C6, RP-D6, RP-CV, RP-DV GR2000-1B/2B	
Main Item	Sub-Item		Input Side	Output Side	Input Side	Output Side	Input Side	Output Side
Designation of operation	Contract band monitoring	-upc <kbps> -upc_burst <Byte>	–	–	–	–	√	√
		-min_rate <kbps> -min_rate_burst <Byte>	–	–	–	–	√	√
		max_rate <kbps> max_rate_burst <Byte>	–	–	–	–	√	√
	Output priority	-priority <No.>	–	–	–	–	√	√
	Queuing priority	-discard <No.>	–	–	–	–	√	√
	DSCP rewrite	-replace_dscp <DSCP_Value>	–	–	–	–	√	√(*1)
	Decision of priority by using DSCP of input IP packet.	-dscp_map	–	–	–	–	√	√
	Abortion at contract band breach.	-penalty_drop	–	–	–	–	√	√
	Queuing priority at contract band breach.	-penalty_discard <No.>	–	–	–	–	√	√
	DSCP rewriting at contract band breach.	-penalty_dscp <DSCP_Value>	–	–	–	–	√	√
	Connection branch	-index <No.>	–	–	–	–	–	√
	Group number	-group<No.>	–	-	-	-	-	√(*2)
	User priority rewrite	-replace_user_priority <No.>	–	–	–	–	–	√

√: Can be set.
-: Cannot be set.
**1): Can be set for uni-cast Cannot be set for multi-cast.*
**2: Can be set only on GR2000-1B, GR2000-2B and GR2000-2B+.*

Action parameters also have parameters decided that can be set according to type of actions. Comparative table is shown below for action parameters that can be set by actions

The flow control type can be divided largely into 11 control types.

- Control 1:

  Determines the priority using the output priority.

- Control 2:

  Determines the priority using the output priority and performs surveillance on the contract band. If the detected flow breaches the contract band, abolishment processing is performed.

- Control 3:

  Determines the priority using the output priority and performs surveillance on the contract band. If the detected flow breaches the contract band, the priority is lowered.

Downloaded from www.Manualslib.com manuals search engine

- Control 4:

  Rewrites DSCP and uses it to determine the priority.
- Control 5:

  Rewrites DSCP, uses it to determine the priority and performs surveillance on the contract band. If the detected flow breaches the contract band, abolishment processing is performed.
- Control 6:

  Rewrites DSCP, uses it to determine the priority and performs surveillance on the contract band. If the detected flow breaches the contract band, the priority is lowered.
- Control 7:

  Determines the priority using the DSCP of the input IP packet.
- Control 8:

  Determines the priority using the DSCP of the input IP packet and performs surveillance on the contract band. If the detected flow breaches the contract band, abolishment processing is performed.
- Control 9:

  Determines the priority using the DSCP of the input IP packet and performs surveillance on the contract band. If the detected flow breaches the contract band, the priority is lowered.
- Control 10:

  Makes allocation to groups.
- Control 11:

  Rewrites user priority.

.

Table 1-47 Operating Parameters that Can Be Set for Each Operation

Operation Parameter	Flow Control										
	1	2(*1)	3(*2)	4	5(*1)	6(*2)	7	8(*1)	9(*2)	10	11
Existence of operating parameter -action	√	√	√	√	√	√	√	√		√	√
Contract band monitoring { -upc <kbps> [-upc_burst <Size>]| -min_rate <kbps> [-min_rate_burst <Byte>]| -max_rate <kbps> [-max_rate_burst <Byte>]| -max_rate <kbps> [-max_rate_burst <Byte>] -min_rate <kbps> [-min_rate_burst <Byte>]}		√	√		√	√		√		√	
Output priority -priority <No.>	x	x	√							x	x
Queuing priority -discard<No.>	x	x	x							x	x
User priority rewrite -replace_user_priority <No.>											√(*6)
Group number -group <No.>										√(*5)	
DSCP rewrite -replace_dscp <DSCP_Value>				√	√	√					

Downloaded from www.Manualslib.com manuals search engine

Table 1-47 Operating Parameters that Can Be Set for Each Operation

Operation Parameter	Flow Control										
	1	2(*1)	3(*2)	4	5(*1)	6(*2)	7	8(*1)	9(*2)	10	11
Priority designation by input IP packet DSCP -dscp_map							√	√	√		
Contract band monitoring -penalty_drop		x (*3)			x (*3)			x (*3)			
Decision of priority by using DSCP of input IP packet. -penalty_discard <No.>			√ (*4)								
Abortion at contract band breach. -penalty_dscp <DSCP_Value>						√ (*4)				√ (*4)	
Output VC and DLCI designation -index <Value>	x	x	x	x	x	x	x	x		x	

√: Indispensable x: Can be set, and default. No mark: Setting is impossible.
**1: This is the operating parameter of contract band monitoring. These conditions cannot be set when "-min_rate<kbps>[-min_rate_burst<Byte>]" is specified. To guarantee the minimum band, this parameter can only change the queuing priority of a packet that violates the contract band.*
**2: This is the operating parameter of contract band monitoring. These conditions cannot be set when only "-max_rate<kbps> [-max_rate_burst<Byte>]" is specified. To limit the maximum band, this parameter can only discard a packet that violates the contract band.*
**3: This is the operating parameter of contract band monitoring. Omit these conditions when "-max_rate<kbps>[-max_rate_burst<Byte>]" is specified.*
**4: This is the operating parameter of contract band monitoring. The operation of a packet that violates the contract band of "-min_rate<kbps>" is specified when "-max_rate<kbps>[-max_rate_burst<Byte>] -min_rate<kbps>[min_rate_burst<Byte>]" is specified.*
**5: No setting is possible on the VLAN line.*
**6: Only VLAN lines can be set. In addition, output priority determination and DSCP rewrite cannot be set simultaneously.*

`<Interface name>`

Description: Specifies the subject interface name set in the ip information or ip-address information. (The ip information or the ip-address information should be set before inputting this command.) RM Ethernet and Tunnel interface are not supported. For details, refer to Table 1-5.

Default: No default is possible.

`{ in | out}`

Description: Specifies the Inbound/Outbound. Either one or both of the Inbound/Outbound can be set against one interface.
in: Inbound (specification of the frame input side)
out: Outbound (specification of the frame output side)

Default: No default is possible.

`[-disable]`

Description: Nullifies the flow control by input/output interface.

Default: Flow control is executed.

`list <List No.>`

Description: Specifies the list number.

Downloaded from www.Manualslib.com manuals search engine

Default: Default is possible only in the indicated case. All the lists are displayed at default.

Range of value: 1 to 20,000 (ten-decimals)

`[list <List No.>-list <list No.>]`

Description: The range of the list number to be treated for display corresponds to the whole list number including IPv4 QoS and IPv6 QoS lists.

Default: The range of the list number to be displayed corresponds to all list numbers.

Range of value: IPv4 QoS list: 1-20000 (decimal)
IPv6 QoS list: 40001-60000 (decimal)

`fee`

Description: Displays the blank list number.

Default: Cannot be omitted when the blank list number is displayed.

`min_no`

Description: Displays the top blank list number in the specified range.

Default: Cannot be omitted when the top list number of a blank list number is displayed.

Flow Detecting Condition Parameters

`{ ip | <protocol No.> | tcp | udp | icmp6 }`

Description: Specifies the high-order protocol number of the protocol name. If all the protocols are taken as the object, ip is specified.

Default: No default is possible.

Range of value: 0 to 255 (ten-decimals). (refer to Table 1-48.) In the case of an IPv6 QoS list, protocol numbers that show the IPv6 option header cannot be designated. Specifically, they are 0 (relay point option header), 43 (route control header), 44 (fragment header) and 60 (terminal point option).

Table 1-48 General Protocol Number

Protocol No.	Protocol
1	ICMP
6	TCP
8	EGP
17	UDP
58	ICMPv6
88	IGRP
89	OSPF

Downloaded from www.Manualslib.com manuals search engine

<IPv6_Source>

Transmitter IPv6 address is designated.

If address to be designated is one:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If address is designated by range:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn -

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If designated by sub-net prefix length:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/aaa

If all IPv6 addresses are designated: any

Default: No default is possible.

Range of value: IPv6 address (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):
0:0:0:0:0:0:0:0-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Prefix length (aaa): 0-128

<IPv6_Destination>

Designated filter conditions by Transmitter IPv6 address.

If address to be designated is

one:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If address is designated by range :

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn -nnnn:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

If designated by sub-net mask length:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/aaa

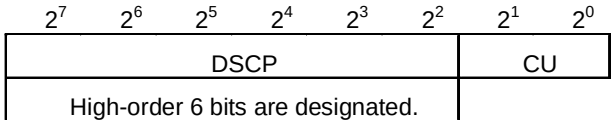
If all IPv6 addresses are designated : any

Default: No default is possible.

Range of value: IPv6 address
(nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):
0:0:0:0:0:0:0:0-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Sub-net mask length (aaa): 0-128

[dscp <DSCP_Value>]

Specifies six high-order bits in the TOS field. Comparison is made on the six high-order bits in the TOS field of the transmission packet. The two low-order bits are ignored even if they are set.



DSCP (Differentiated Services Code Point), CU (Current Unused)

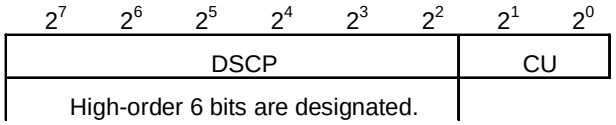
Default: None. (DSCP value is not included in the flow detecting condition.

Range of value: 0-63 (10-decimals)

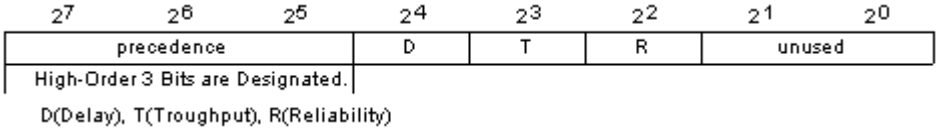
Downloaded from www.Manualslib.com manuals search engine

[precedence <precedence_Value>]

This parameter specifies precedence value, which is the upper 3 bits of the ToS field. This is compared to the upper 3 bits of the ToS field of sent/received packets. The lower 5 bits of the ToS field are ignored.



DSCP (Differentiated Services Code Point), CU (Current Unused)



Default: None (precedence values are not included in the detecting condition)

Range of value: 0 - 7 (decimal)

[{ upper | lower } <Length>

Specifies the upper or lower limit of the IP user data length.

-upper: Upper limit of the IP user data length is designated.

-lower: Lower limit of the IP user data length is designated.

Default: None (TOS values are not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal).

Table 1-49 Relationship Between Upper and Lower IP User Data Length Limits and IP User Data Length

Upper and Lower Limits Designation	Relationship between A (packet value) : (Total Length) - (Header Length)) and B (IP user data length designated in constituting definition information)	Result
-upper	A ≤ B	Agreed.
-upper	A > B	Disagreed.
-lower	A ≥ B	Agreed.
-lower	A < B	Disagreed.

[<port_source>]

Specifies the transmitter port number.

If port to be specified is one: nnnnn

If port number is specified by range:nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-50.)

Downloaded from www.Manualslib.com manuals search engine

[<port_destination>]

Specifies the destination port number.

If port to be specified is one: nnnnn

If port number is specified by range:nnnnn-nnnnn

Default: None (the transmitter port number is not included in the flow detecting condition.)

Range of value: 0 to 65535 (decimal). (Please refer to Table 1-50.)

Table 1-50 General ICMP Type Code Number

Port Number (Decimal)	Name
20/tcp	File Transfer [Default Data]
21/tcp	File Transfer [Control]
22/tcp	Secure Shell Login
23/tcp	Telnet
25/tcp	Simple Mail Transfer
53/tcp 53/udp	Domain Name Server
80/tcp	World Wide Web HTTP
110/tcp 10/udp	Post Office Protocol - Version 3
161/udp	SNMP

[<ICMPv6_Type>]

Description: Specifies the IGMPv6 type.

Default: None.(The IGMPv6 type is not included in the flow detecting condition.)

Range of value: 0 to 255 (ten-decimals). (Please refer to Table 1-51.)

[<ICMPv6_Code>]

Description: Specifies the IGMPv6 type.

Default: None.(The IGMPv6 type is not included in the flow detecting condition.)

Range of value: 0 to 255 (ten-decimals). (Please refer to Table 1-51.)

Table 1-51 General IGMPv6 Type Code Number

Type	Name	Code
1	Destination Unreachable	0 - 4
2	Packet Too Big	0
3	Time Exceeded	0 - 1
4	Parameter Problem	0 - 2
128	Echo	0
129	Echo Reply	0
130	Multicast Listener Query	0
131	Multicast Listener Report	0
132	Multicast Listener Done	0
133	Router Solicitation (NDP)	0

Downloaded from www.Manualslib.com manuals search engine

Table 1-51 General IGMPv6 Type Code Number

Type	Name	Code
134	Router Advertusement (NDP)	0
135	Neighbor Solicitation (NDP)	0
136	Neighbor Advertusement (NDP)	0
137	Redirect (NDP)	0

`[user_priority <No.>]`

Description: Specifies user priority. This parameter specify "in"(Inbound) VLAN line information.

Default: None

Range of value: 0 -7

`Ordinary packet flow detecting condition} [premium {important packet flow detecting condition}]`

When the maximum band restriction (-max_rate) or the minimum band assurance (-min_rate) is executed, the important packet is transferred with priority given in the band, and the ordinary packet is transferred when the important packet is not transferred by using all the bands. This function is called the important packet assuring function. The flow detecting conditions for the ordinary packet are inputted before the premium, and the flow detecting conditions for the important packet after the premium. The flow detecting conditions for the important packet can be set only after either one of the maximum band restriction (-max_rate) or the minimum band assurance (-min_rate) has been set.

The parameters that have not been set in the important packet flow detecting conditions are subjected to the same conditions as the parameters that have been set in the ordinary packet flow detecting conditions. For setting the important packet flow detecting conditions, set only the flow detecting condition parameters whose detecting conditions differ from the ordinary packet flow detecting conditions.

When the important packet protecting function is used, the number of entries used per list becomes two or four entries.(Note 3)

Default: None. (The important packet protecting function is not used.)

Range of value: None

Operation Parameters

`[-action]`

If the operation parameter is either set or changed, please be sure to set this parameter at the head of the whole operation parameter.

Default: None (No default is possible when designating the operation.)

Range of value: None

`[-upc <kbps> [-upc_bu st <Byte>]]`

Specifies the contract band by kbit/s. Specifies burst size in byte unit. If a value greater than the line speed is set, no action at breach is taken.

When setting this parameter, it is not possible to set -max_rate, -max_burst, and min_rate_rate, -min_rate_burst. (-upc_burst is effective only in RP-C and RP-D.)

Default: None. (No contract band surveillance is executed.)

Downloaded from www.Manualslib.com manuals search engine

Range of value: <kbps> : 0 to 2400000 (0 to 2.4G) (10-decimals).

If 0 to 4 is specified in the case of RP-C and RP-D, the operation is performed by taking the contract band as 4.1[kbit/s].

<Byte> : 0 to 131072 (10-decimals)

`[-max_ rate <kbps> [-max_ rate_bust <Byte>]]`

Specifies the maximum contract band restriction by kbit/s. Specifies burst size in byte unit. If a value greater than the line speed is set, no action at breach is taken.

When setting this parameter, it is not possible to set -upc, or -upc_burst.

Packets exceeding the maximum band when setting this parameter are all discarded.

When this is used, the number of entries used per list may become two or four entries.(Note 1)

Default: None. (No contract band surveillance is executed.)

Range of value: <kbps> : 0 to 2400000 (0 to 2.4G) (10-decimals).

If 0 to11 is specified in the case of RP-A, the operation is performed by taking the contract band as 12[kbit/s].

If 0 to 4 is specified in the case of RP-C and RP-D, the operation is performed by taking the contract band as 4.1[kbit/s].

<Byte> : 0 to 131072 (10-decimals)

`[-min_ rate <kbps> [-min_ rate_bu st <Byte>]]`

Specifies the minimum band assurance by kbit/s. Specifies burst size in byte unit.

If a value greater than the line speed is set, no action at breach is taken.

When setting this parameter, it is not possible to set -upc, or -upc_burst.

When this parameter is used, the number of entries used per list may become two or four entries. (Note 1)

Default: None. (No contract band surveillance is executed.)

Range of value: <kbps>: 0 to 2400000 (0 to 2.4G) (10-decimals).

If 0 to 4 is specified, the operation is performed by taking the contract band as 4.1[kbit/s].

<Byte>: 0 to 131072 (10-decimals)

`[-index <No.>]`

Specifies the connection branching index number (index specified in the DLCI group information or the Vc-Group information). It selects and transmits DLCI/VC specified in the group when relaying the packet that agrees with the flow detecting conditions. For the list information setting the connection branching index number, specify out (Outbound) as the flow control of the output side.

Default: None.

Range of value: 0 to 7.

Downloaded from www.Manualslib.com manuals search engine

[-priority <No.>] [-discard <No.>]

Makes the flow control function effective by specifying the output priority and queuing priority. Sets the priority in <No.>. The priority parameter is used as the output priority in the case of output priority control and as the queue number in the case of minimum band assurance. If the output line is an ATM line, it sets the value of the cell loss priority indication (CLP bit) of the cells transmitting in VC using either the "output" priority or the "queuing" priority. To set the cell loss indication bit, refer to the parameters defined in the *GR2000 Configuration Commands, (universal CLI) Vol. 1*, vc (VC information)." If the VC's service category is GRR or GFR2, select the "queuing" priority from the VC priority queue. If the VC's service category is GFR2, set the output priority from the VC priority queue. For the queuing and output priority of VC priority queuing, refer to the *GR2000 Applications Guide*. When setting this parameter, it is not possible to set -replace_dscp, or -class_dscp.

Default: -priority: 4
-discard: 4

Range of value: -priority <No.>: 1 to 1000

(Incase of the output priority control, the greater the value of the output priority, the more preferentially the packet is issued.)

-discard <No.>: 1 to 4.
(The smaller the value of the queuing priority, the more preferentially the packet is discarded.)

The ranges for the output priority (priority) and the queuing priority(discard)vary depending on the setting conditions.

Table 1-52 Relationship Between Number of Queues and Priority Setting Condition Range

Setting Condition		Range	
Interface Using this List	**No. of Queue in Output Interface**	**Output Priority (*1)**	**Queuing Priority**
Input side	--	1 - 8	1 - 4
Output side	4	1 - 4	1 - 4
Output side	8	1 - 8	1 - 4
Output side	16	1-16	1 -4
Output side	32	1 - 32	1 - 4
Output side	64	1 - 64	1 - 4
Output side	250	1 - 250	1 - 4 (*2)
Output side	1000	1 - 1000	1 - 4 (*2)

**1: If value outside the range is set in output priority, the setting contents are nullified.*
**2: If the QoS attribute of the output interface is the minimum band assurance (specified by kbit/s), the flow control is executed as follows:*
- *Queuing priority 1 and 2: Flow control is executed at queuing priority 2.*
- *Queuing priority 3 and 4: Flow control is executed at queuing priority 4.*

[-group<No.>][ROUTE-OS6B]

Designates the group number to be outputted when the output line transmission control is the group band control relative to the Line. Setting is possible only when the group number has been previously set in the QoS interface

Downloaded from www.Manualslib.com manuals search engine

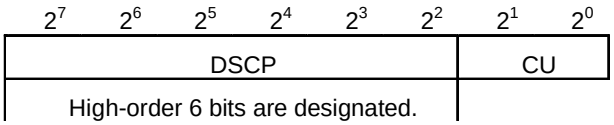
information. Designate this parameter's out (Outbound) as the flow control of the output side. When this parameter is designated, only "-priority" and "-discard" can be set. The setting range for "-priority" is from one to four. This parameter cannot be set if the output line is a VLAN line.

Default None

Range of value The group number designated by the qos-interface (QoS interface information).

[- replace_dscp <DSCP_Value>]

This parameter enables the function that rewrites a DSCP value and that determines the output priority and queuing priority using the rewritten DSCP value. The DSCP value and its corresponding output priority and queuing priority are specified using a *qos-tos-map* command. This parameter rewrites the DSCP value that is the upper six bits of a TOS field. The lower two bits of a TOS field are not rewritten. On the output side, do not specify this parameter to multicast packets.



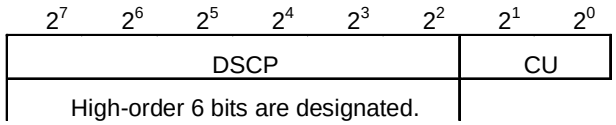
DSCP (Differentiated Services Code Point), CU (Current Unused)

Default: -priority: 4
-discard: 4
(Flow control when output priority and queuing priority are specified.)

Range of value: - replace_dscp<DSCP_Value>:0-255(decimal) (Note 1, 2)

[-dscp_map]

This parameter enables the function that determines the output priority and queuing priority using the DSCP value of an input packet. The DSCP value and its corresponding output priority and queuing priority are specified using a qos-tos-map command. The upper six bits of a TOS field in a receive packet are treated as a target. The lower two bits of a TOP field are ignored. -priority, -discard, and -replace_dscp cannot be set when this parameter is set.



DSCP (Differentiated Services Code Point), CU (Current Unused)

Default: -priority: 4
-discard: 4
(Flow control when output priority and queuing priority are specified.)

[{-penalty_drop | -penalty_disca d <No.> | -penalty_dscp <DSCP_Value>}]

Specifies the operation when the contract band is breached.

-penalty_drop: Packet discard.

-penalty_discard <No.>:

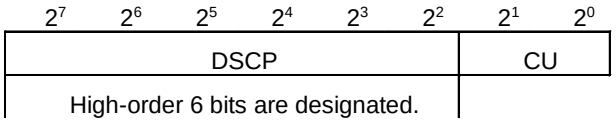
Downloaded from www.Manualslib.com manuals search engine

Specifies the queuing priority after having been changed. If this parameter is specified and the output line is ATM, it is possible to set the cell loss priority indication bit (CLP bit) of a cell transmitted by VC to zero when the queuing priority is three or four, and to one when the queuing priority is one or two. For setting the cell loss indication bit, please refer to in *GR2000 Configuration Commands, (universal CLI) Vol. 1*.

`-penalty_ dscp <DSCP_Value> :`

Specifies the DSCP rewriting value and controls QoS by using the rewritten DSCP.

However, what is rewritten is the six high-order bits in the DSCP field. The two low-order bits are ignored even if they are set.



DSCP(Differentiated Services Code Point), CU(Current Unused)

Default: When setting -upc: -penalty_drop
When setting -max_rate: -penalty_drop (Packets breaching the maximum band are all discarded.)
When setting -min_rate: -discard 1 (Packets breaching the minimum band are discarded more easily.)

Range of value: -penalty_dscp <DSCP_Value>: 0 to 63 (decimals)

-penalty_discard <No>: 1-4
(The smaller the value of the queuing priority, the more preferentially the packet is discarded.)

Table 1-53 Relationship between number of queues and priority

Setting Condition		Range
Interface Using this List	**No. of Queue in Output Interface**	**Queuing Priority**
Input side	--	1-4
Output side	4	1-4
Output side	8	1-4
Output side	16	1-4
Output side	32	1-4
Output side	64	1-4
Output side	250	1-4 (*2)
Output side	1000	1-4 (*2)

**1: If value outside the range is set in output priority, the setting contents are nullified.*
**2: If the QoS attribute of the output interface is the minimum band assurance (specified by kbps), the flow control is executed as follows:*
- *Queuing priority 1 and 2: Flow control is executed at queuing priority 2.*
- *Queuing priority 3 and 4: Flow control is executed at queuing priority 4.*

Note: Depending on setting of the important packet protection function, maximum band restriction and minimum band guarantee, the number of entry used per list will be the number of entry used per list for each setting as shown in Table 1-54.

Downloaded from www.Manualslib.com manuals search engine

-replace_user_priority <No.>

Specifies the rewriting value for user priority.

Use this parameter to specify "out" (outbound) VLAN line information as flow control on the outbound side. When this parameter is set, it is only possible to set -priority, -discard and -replace dscp.

Default: None

Range of value: 0 - 7

Table 1-54 Number of Entries Used per List by Each Setting

Setting Contents	Setting Parameter			Number of Entry
	premium	*-max_rate*	*-min_rate*	
No setting				1
Maximum band restriction		√		1
Minimum band assurance			√	1
Maximum band restriction + minimum band assurance		√	√	2
Maximum band restriction + important packet protection	√	√		2
Minimum band assurance + important packet protection	√		√	2
Maximum band restriction +minimum band assurance +important packet protection	√	√	√	4

√: With setting. No mark : Without setting

Examples

1. Setting the QoS flow information:
   Classification of packets
   In order to preferentially transfer the packets with the transmitter IPv6 addresses of 3ffe::501:811:ff01:1::1, the high-order protocol of TCP, and with the destination port number of 23 (telnet), the output priority class of the said packets are specified as seven and that of other packets as one.

```
(config)#  flow qos Tokyo out list 40001 tcp 3ffe:501:811:ff01:1::1 any 23
-action -priority 7
(config)#   flow qos Tokyo out list 60000 ip any any action priority 1
(config)#   flow yes
(config)#   show flow
flow yes {
        qos Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
priority 7;
                list 60000 ip any any action priority 1;
        };
};
(config)#
```

   Specification of contract band:

   Specify so that the traffic from the end users can be monitored by using ISP, and the packets breaching the contract band will be aborted. Specify so that the packet whose transmitter IPv6 address in the input interface name of Tokyo is 3ffe:501:811:ff01:1::1 can be monitored by the contract band 128 kbit/s.

Downloaded from www.Manualslib.com manuals search engine

```
(config)#   flow qos Tokyo in list 40001 ip 3ffe:501:811:ff01:1::1 any
-action -upc 128
(config)#   flow -yes
(config)#   show flow
flow yes {
        qos Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action upc 128;
        };
};
(config)#
```

Specification of queuing priority when contract band is breached:

Specifies that packets breaching the contract band be discarded more easily when the output lines are congested. Monitors the packets with the interface name of Tokyo and the transmitter address of 3ffe::501:811:ff01:1::1 in the contract band of 5,000 kbit/s and changes the queuing priority to one at breach.

```
(config)#   flow qos Tokyo in list 40001 ip 3ffe:501:811:ff01:1::1 any
-action -upc 5000 -penalty_discard 1
(config)#   flow -yes
(config)#   show flow
flow yes {
        qos Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action upc 5000
penalty_discard 1;
        };
};
(config)#
```

Specifying the maximum band restriction plus minimum band assurance:

Sets the maximum band restriction and the minimum band assurance by each end user by using ISP. Specifies the users with the interface name of Tokyo and the transmitter addresses of 3ffe::501:811:ff01:1::1 and 3ffe::501:811:ff02:1::1 with the maximum band restriction band of 128 kbit/s and the minimum band assurance band of 64 kbit/s.

```
(config)#   flow qos Tokyo out list 40001 ip any 3ffe:501:811:ff01:1::1
-action -max_rate 128 -min_rate 64
(config)#   flow qos Tokyo out list 40002 ip any 3ffe:501:811:ff02:1:: -
action -max_rate 128 -min_rate 64
(config)#   flow -yes
(config)#   show flow
flow yes {
        qos Tokyo out {
                list 40001 ip any 3ffe:501:811:ff01:1::1 action max_rate
128 min_rate 64;
                list 40002 ip any 3ffe:501:811:ff02:1::1 action max_rate
128 min_rate 64;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Specifying the maximum band restriction plus minimum band assurance plus important packet protecting function:

Sets the maximum band restriction, the minimum band assurance, and important packet protecting function for each end user by using ISP. Specifies that the users with the interface name of Tokyo and the transmitter address of 3ffe::501:811:ff01:1::1 have a maximum band restriction band of 128 kbit/s and the minimum band assurance band of 64 kbit/s, gives the important packet a TOS value of 10, and the other packets TOS values different from that.

```
(config)#   flow qos Tokyo out list 40001 ip any 3ffe:501:811:ff01:1::1
premium ip any any dscp 10 -action -max_rate 128 -min_rate 64
(config)#   flow -yes
(config)#   show flow
flow yes {
        qos Tokyo out {
              list 40001 ip any 3ffe:501:811:ff01:1::1 premium ip any any
dscp 160 action max_rate 128 min_rate 64;
        };
};
(config)#
```

Connects two bases by two VCs, and allots them to separate VCs according to flow:

Allots the VC with the connection branching index number one to packets whose transmitter IPv6 addresses are 3ffe::501:811:ff01:1::1 to 3ffe::501:811:ff0f:1::1, and the VC with the connection branching index number zero to packets with the transmitter addresses other than those above.

```
(config)#   flow qos Tokyo out list 40001 ip
3ffe:501:811:ff01:1::1-3ffe:501:811:ff0f:1::1 any -action -index 1
(config)#   flow qos Tokyo out list 40002 ip any any -action -index 0
(config)#   flow -yes
(config)#   show flow
flow yes {
        qos Tokyo out {
             list 40001 ip 3ffe:501:811:ff01:1::1-3ffe:501:811:ff0f:1::1
any action index 1;
                list 40002 ip any any action index 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

DSCP value rewriting:

Rewrites the DSCP value according to each traffic flow received from end users.

Rewrites the DSCP value of the packets with the transmitter IPv6 address of 3ffe::501:811:ff01:1::1 to 34 and those with 3ffe::501:811:ff02:1::1 to 10.

```
(config)#   flow qos Tokyo in list 40001 ip 3ffe:501:811:ff01:1::1 any
-action -replace_dscp 34
(config)#   flow qos Tokyo in list 40002 ip 3ffe:501:811:ff02:1::1 any
-action -replace_dscp 10
(config)#   flow -yes
(config)#   show flow
flow yes {
        qos Tokyo in {
                list 40001 ip 3ffe:501:811:ff01:1::1 any action
replace_dscp 34;
                list 40002 ip 3ffe:501:811:ff02:1::1 any action
replace_dscp 10;
        };
};
(config)#
```

2. Inserting the list:
   The list number 40003 is inserted between the list numbers 40001 and 40005.

```
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
priority 7;
                list 40005 ip any any action priority 1;
        };
};
(config)#   flow qos Tokyo out list 40003 tcp any any -action -priority 4
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
priority 7;
                list 40003 tcp any any action priority 4;
                list 40005 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Nullification of QoS flow information by each input/output interface:
   Nullifies the QoS flow control of the output interface Tokyo.

```
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
priority 7;
                list 40005 ip any any action priority 1;
        };
};
(config)#   flow qos Tokyo out -disable
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out disable {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
priority 7;
                list 40005 ip any any action priority 1;
        };
};
(config)#
```

4. Changing the parameter and changing the parameters for flow detecting conditions and operation specification:
   Changes the parameters for flow detecting conditions and operation specification in the list of the list number 40001.

```
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 tcp 3ffe:501:811:ff01:1::1 any 23 action
priority 7;
                list 5 ip any any action priority 1;
        };
};
(config)#   flow qos Tokyo out list 40001 udp 3ffe:501:811:ff01:1::1 any
-action -priority 6
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
               list 40001 udp 3ffe:501:811:ff01:1::1 any action priority
6;
                list 40005 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Changing only the parameter for operation specification:

Changes the parameters in the list of the list number 40001 from the output priority of six to the output priority of two.

```
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 udp 3ffe:501:811:ff01:1::1 any action priority
6;
                 list 40005 ip any any action priority 1;
        };
};
(config)#   flow qos Tokyo out list 40001 action priority 2
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 udp 3ffe:501:811:ff01:1::1 any action priority
2;
                 list 40005 ip any any action priority 1;
        };
};
(config)#
```

5. Deleting the QoS flow information and deleting the input/output interface unit:
   Deletes the QoS flow information of the input/output interface Tokyo.

```
(config)#   show flow qos
flow yes {
        qos Tokyo in {
                 list 40001 ip 3ffe:501:811:ff01:1::1 any action
replace_dscp 40;
        };
        qos Tokyo out {
               list 40001 ip any 3ffe:501:811:ff01:1::1 action priority 2;
                 list 40005 ip any any action priority 1;
        };
};
(config)#   delete flow qos Tokyo out
(config)#   show flow qos
flow yes {
        qos Tokyo in {
                 list 40001 ip 3ffe:501:811:ff01:1::1 any action
replace_dscp 40;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Deleting the list unit:

Deletes the list number one of the input/output interface Tokyo.

```
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
               list 40001 ip any 3ffe:501:811:ff01:1::1 action priority 2;
                list 40005 ip any any action priority 1;
        };
};
(config)#   delete flow qos Tokyo out list 40001
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40005 ip any any action priority 1;
        };
};
(config)#
```

Deleting the parameters for operation specification:

Deletes the operation specification in the list number one of the input/output interface Tokyo.

```
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
               list 40001 ip any 3ffe:501:811:ff01:1::1 action priority 2;
                list 40005 ip any any action priority 1;
        };
};
(config)#   delete flow qos Tokyo out list 40001 -action
(config)#   show flow qos Tokyo out
flow yes {
        qos Tokyo out {
                list 40001 ip any 3ffe:501:811:ff01:1::1 ;
                list 40005 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Displaying the QoS flow information and displaying all the input/output interface:
   Displays the QoS flow information for the entire input/output interface.

```
(config)#   show flow qos
flow yes {
        qos Tokyo in {
              list 40001 ip 3ffe:501:811:ff01:1::1 any action replace_dscp
40;
        };
        qos Osaka out {
               list 40001 ip any 3ffe:501:811:ff02:1::1 action priority 2;
                list 40005 ip any any action priority 1;
        };
};
(config)#
```

   Displaying the input/output interface unit:

   Displays the QoS flow information for the input/output interface Osaka.

```
(config)#   show flow qos Osaka out
flow yes {
        qos Osaka out {
               list 40001 ip any 3ffe:501:811:ff01:1::1 action priority 2;
                list 40005 ip any any action priority 1;
        };
};
(config)#
```

   Displaying the list unit:

   Displays the QoS flow information of the list number five for the input/output interface Osaka.

```
(config)#   show flow qos Osaka out list 40005
flow yes {
        qos Osaka out {
                list 40005 ip any any action priority 1;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

7. Display of blank list number
   Display of all blank list numbers
   Display all blank list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#   show flow qos Tokyo in free
Free number(IPv4): 5,7,15-20000
Free number(IPv6): 40002-60000
(config)#
```

Display of blank list number in the specified range:

Display all blank list numbers in the range in which the list number is 40001 to 40100 on the Inbound (input) side of interface Tokyo.

```
(config)#   show flow qos Tokyo in list 40001-40100 free
Free number(IPv6): 40002-40100
(config)#
```

Display of top blank list number in all list numbers:

Display the top blank list number in the list numbers on the Inbound (input) side of interface Tokyo.

```
(config)#   show flow qos Tokyo in free min_no
Free number(IPv4): 5
Free number(IPv6): 40001
(config)#
```

Display of top blank list number in the specified range:

Display the top blank list number in the range in which the list number is 40051 to 40100 on the Inbound (input) side of interface Tokyo.

```
(config)#   show flow qos Tokyo in list 40051-40100 free min_no
Free number(IPv6): 40051
(config)#
```

Related Commands

flow, flow filter, qos, qos-tos-map, qos-ip-list, filter-list, nat, nat inside interface, nat outside interface

Related Information

For the flow control, please refer to the *GR2000 Applications Guide*.

Downloaded from www.Manualslib.com manuals search engine

Precautions

1. Determination of the QoS flow is performed in the order of the list number specified in the input/output interface in the QoS flow information (the order of display when show flow qos is executed).
2. When setting the qos-ip-list (QoS IP frame condition information) or filter-list (filter list information), this command cannot be set. Delete both qos-ip-list and filter-list before setting this command.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
4. Flow information consumes 101 entries in each RP when address conversion (nat) is set. Therefore, when address conversion (nat) is set, the maximum entry count is decreased by 101 per RP capable of flow information definition.

Table 1-55 Features of Constituting Definition of Filter Flow Information by Input Form

Item	Constituting Definition Inputting Form	
	qos-ip-list, qos-ip-list-group,qos-ip	***flow filter***
Number of entry(*1)	1024 entry/device	10000 entry/device 2000 entry/RP
Inputting form	Input three commands to define one list. Effective in defining the same flow control in multiple number of input/output interfaces.	Input one command to define one list. Effective in inputting a number of entries.
Function use, and unused unit	Device unit	Device unit, and input/output interface unit
GR2000 Operations Commands, Vol. 2 - Indication unit for show qos ip-flow.	Device unit and list unit	Device unit and input/output interface unit
Vacant entry indication	Supported.	Unsupported.
**1: Total value with entries of filters.*		

Downloaded from www.Manualslib.com manuals search engine

1.1.10 filter

Function

Object for creation, modification, deletion, and display of the filter information. The filter function forwards or discards packets that match a specific condition and forwards all packets that do not match the condition.

Input Format

To create or modify the filter information:

```
[set] filter [ { -no | -yes } ] [ { -deny_own | -deny_own_off } ]
```

To delete the filter information:

```
delete filter
```

To show the filter information:

```
show filter
```

Parameter

`{ -no | -yes }`

Description: Specifies whether to use the filter function.

Default: No

`{ -deny_own | -deny_own_off }`

Description: Specifies whether to filter the receipt packet addressed to this router.

Default: -deny_own_off

Range of value: None

Examples

1. Enabling filtering:

```
(config)#: filter -yes
(config)# show filter
filter yes;
(config)#
```

2. Enabling filtering of receipt packet addressed to this router:

```
(config)# filter -deny_own
(config)# show filter
filter yes {
         deny_own;
}; (config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Show the current filter settings, modify the filter information so as not to use the filter, and show the result:

```
(config)# show filter
filter yes {
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
filter_group fil1 {
filter_list 1;
};
filter_interface ip2 out filter_group fil1;
};
(config)# filter no
(config)# show filter
filter no {
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
filter_group fil1 {
filter_list 1;
};
filter_interface ip2 out filter_group fil1;
};
(config)#
```

4. Delete the filter:

```
(config)# delete filter
Are you sure? (y/n):y
(config)#
```

5. Delete the specified parameter and reset to the default value. Delete the filter of receipt packet addressed to this router:

```
(config)# show filter
filter yes {
         deny_own;
};
(config)# delete filter -deny_own
(config)# show filter
filter yes;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Configuration Object

```
filter-list
filter-group
filter-interface
```

Precautions

1. Use the filter command with the set subcommand must precede that of the related command shown above. If the filter information is set once, further input is enabled as long as the filter information is not deleted.
2. When the filter information is defined, applicable parameters of the `filter-list` object, `filter-group` object, and `filter-interface` object must also be defined.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.1.11 *filter-list* (Filter List Information in the Old BSD UNIX-Based Command System)

Function

Object for creation, modification, deletion, and display of the filter list information. The filter list determines whether to forward or discard packets that match a specific condition. Packets not matching such a condition are forwarded. A maximum of 1024 filter list entries (filter conditions) can be created per device.

Input Format

To create or modify the filter list information:

```
[set] filter-list <Filter List No.> [{ -forward | -drop }] [-protocol
<No.>] [{ -payload_length_upper_limit <Payload Length> |
-payload_length_lower_limit <Payload Length>}][-tos <Value>][{ -ip_pair |
-ip_pair_off }][-ip_source <IP Address> [-<IP Address> | mask <Subnet
Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]]
[-ip_destination <IP Address>  [-<IP Address> | mask <Subnet Mask> |
masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]] [{
-port_pair | -port_pair_off }] [-port_source <Port No.> [-<Port No.>]]
[-port_destination <Port No.> [-<Port No.>]] [{ -pair_synchronized_off |
-pair_synchronized }] [{ -ack_check_off | -ack_check }] [{ -syn_check_off
| -syn_check }]  [-icmp_type <No.>] [-icmp_code <No.>] [-igmp_type <No.>]
[-branch_index <No.>] [-policy_routing <Interface Name> <IP Address>]
[-policy_routing-group <policy-Group-Name] [-replace_tos <New Tos>]
```

To delete the filter list information:

```
delete filter-list <Filter List No.>
```

To show the filter list information:

```
show filter-list [<Filter List No.>]
```

To show all of the free entry No.:

```
show filter-list free
```


Downloaded from www.Manualslib.com manuals search engine

To show the first free entry No.:

```
show filter-list free min_no
```

Parameters

Filters can be set based on information in the TCP, UDP, ICMP, IGMP packets. See Table Table 1-56 for a list of parameters and conditions.

Table 1-56 Applicable Parameters by Upper Protocol

Parameter	TCP	UDP	ICMP	IGMP	Undefined
Filter list no.	§	§	§	§	§
-forward | -drop	u	u	u	u	u
-protocol <No.>	6	17	1	2	°
-payload_length_upper_limit <Payload Length> | -payload_length_lower_limit <Payload Length>	°	°	°	°	°
-tos <Value>	°	°	°	°	°
-ip_pair | -ip_pair_off	u	u	u	u	u
-ip_source <IP Address> [-<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]	°	°	°	°	°
-ip_destination <IP Address> [-<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]	°	°	°	°	°
-port_pair | -port_pair_off	u	u			
-port_source <Port No.> [-<Port No.>]	°	°			
-port_destination <Port No.> [-<Port No.>	°	°			
-pair_synchronized_off | -pair_synchronized	u	u			
-ack_check_off | -ack_check	u				
-syn_check_off | -syn_check	u				
-icmp_type <No.>			°		
-icmp_code <No.>			°		
-igmp_type <No.>				°	
-branch_index <No.>	°	°	°	°	°
-policy_routing <Interface Name> <IP Address>	°	°	°	°	°
policy_routing-group <policy-Group-Name>-	°	°	°	°	°
-replace_tos <New Tos>	°	°	°	°	°

§=must be set
°=can be set
u=can be set; default when omitted
No symbol =cannot be set
Number=set number

`<Filter List No.>`

Description: Specifies the filter list number.

Default: Undefined (mandatory input except when used with show subcommand).

Range of value: `1-1024`

Downloaded from www.Manualslib.com manuals search engine

`{ -forward | -drop }`

Description: Specifies the operation when the packet matches the filter condition. The `-forward` option forwards matching packets and the `-drop` option discards the matching packets.

Default: Forward

`-protocol <No.>`

Description: Specifies the upper protocol number in decimal. Upper protocols include TCP, UDP, ICMP, and IGMP.

Default: Undefined

Range of value: 0–255

`{-payload_length_upper_limit <Payload Length> |-payload_length_lower_limit <Payload Length>}`

Description: Specifies the upper or lower limit of the IP user data length (value of total packet length minus header length in bytes). Table 1-57 shows the relationships between such upper and lower limits and the resulting user data length. In this table, “A” indicates the packet length excluding the header length, and “B” indicates the IP user data length.

Default: None

Range of value: 0–65535.

Table 1-57 Filtering Condition Derived from Relation between Limit Setting Parameter and IP User Data Length

Limit Setting Parameter	Relation between Packet Length and IP User Data Length	Filtering Condition
-payload_length_upper_limit	A < or = B	Match
-payload_length_upper_limit	A > B	Mismatch
-payload_length_lower_limit	A > or = B	Match
-payload_length_lower_limit	A < B	Mismatch

`-tos <Value>`

Description: Specifies the value of high-order 6 bits in the TOS field and compares with the high-order 6 bits in the TOS field of receipt packet. The low-order 2 bits are ignored.

Table 1-58 Corresponding Values - *tos <Value>*

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Precedence			D	T	R	Unused	
The six high-order bits are specified. *D = delay T = throughput R = reliability*							

This parameter is used at specifying the high-order 6 bits in the DS field of Diff-serv by the same condition with TOS field.

Downloaded from www.Manualslib.com manuals search engine

Table 1-59 Corresponding Values - *Diff-serv*

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
DSCP						CU	
The six high-order bits are specified. *DSCP* = *Differentiated Services Code Point* *CU* = Currently Unused							

Default: None (Does not include TOS value to the condition of flow detection.)

Range of value: 0-255

`{-ip_pair | ip_pair_off}`

Description: Specifies the method of checking the transmission source IP address and the destination IP address. The `-ip_pair` option checks for both switching as well as non-switching source IP address with destination IP address (see Note later in this subsection). The `-ip_pair_off` option only checks for not switching source IP address with destination IP address. The `-ip_pair` option requires setting of the synchronized pair switch for the IP address upper protocol port number to off (`-pair_synchronized_off`).

Default: On

`-ip_source <IP Address>[-<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]`

Description: Specifies the source IP address. When both source and destination IP addresses are set under one condition, set so that the specified addresses do not overlap. If they overlap, set an IP address pair switch as ip-pair_off. (Note 1)

When specifying only one IP address: `-ip_source <IP Address>`

When specifying addresses within a range:

Specify the lower limit and upper limit of IP addresses:
`-ip_source <IP Address>-<IP Address>`

Specify the subnet mask:
`-ip_source mask <Subnet Mask>`

Specify the subnet mask length:
`-ip_source masklen <Subnet Mask Bit Length>`
or
`-ip_source/<Subnet Mask Bit Length>`

You cannot directly modify the subnet mask or the subnet mask length for only one IP address. You must first delete the setting by entering `delete filter-list <Filter List No.> -ip_source` and then specify the IP address.

Default: Undefined

Range of value: IP address: 0.0.0.0–255.255.255.255
Subnet mask: 255.0.0.0–255.255.255.255
Subnet mask bit length: 8–32

Downloaded from www.Manualslib.com manuals search engine

`-ip_destination<IP Address>[-<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]`

Description: Specifies the destination IP address. When both destination and source IP addresses are set under one condition, set so that the specified addresses do not overlap. If they overlap, set an IP address pair switch as ip-pair_of. (Note 1)

When specifying only one IP address: `-ip_destination <IP Address>`

When specifying addresses within a range:

Specify the lower limit and upper limit of IP addresses:
`-ip_destination <IP Address>-<IP Address>`

Specify the subnet mask:
`-ip_destination mask <Subnet Mask>`

Specify the subnet mask length:
`-ip_destination masklen <Subnet Mask Bit Length>`
or
`-ip_destination/<Subnet Mask Bit Length>`

You cannot directly modify the subnet mask or the subnet mask length for only one IP address. You must first delete the setting by entering `delete filter-list <Filter List No.> -ip_destination` and then specify the IP address.

Default: Undefined.

Range of value: IP address: 0.0.0.0–255.255.255.255
Subnet mask: 255.0.0.0–255.255.255.255
Subnet mask bit length: 8–32

`{-port_pair | -port_pair_off}`

Description: Specifies the method for checking the source upper protocol port number and the destination upper protocol port number. The `-port_pair` option checks for not switching and for switching source upper protocol port number with destination upper protocol port number (see Note later in this subsection). The `-port_pair_off` option only checks for not switching source upper protocol port number with destination upper protocol port number. The `-port_pair` option requires setting of the synchronized pair switch for the IP address upper protocol port number to off (`-pair_synchronized_off`).

Default: On

`-port_source <Port No.>[-<Port No.>]`

Description: Specifies the source upper protocol port number. When both source and destination upper protocol port numbers are set under one condition, set so that the specified upper protocol port numbers do not overlap. If they overlap, set an upper protocol port number's pair switch as -port_pair_off. (Note 1)

When specifying only one port number:
`-port_source <Port No.>`

Downloaded from www.Manualslib.com manuals search engine

When specifying port numbers within a range:
`-port_source <Port No. > -<Port No. >`

Default: Undefined

Range of value: 0–65535

`-port_destination <Port No.>[-<Port No.>]`

Description: Specifies the destination upper protocol port number. When both destination and source upper protocol port numbers are set under one condition, set so that the specified upper protocol port numbers do not overlap. If they overlap, set an upper protocol port number's pair switch as -port_pair_off. (Note 1)

When specifying only one port number:
`-port_destination <Port No.>`

When specifying port numbers within a range:
`-port_destination <Port No. > -<Port No. >`

Default: Undefined

Range of value: 0–65535

`{-pair_synchronized_off | pair_synchronized}`

Description: Specifies the synchronization check method for the IP address and the upper protocol port number as follows:

`-pair_synchronized_off`: Only checks for not switching source IP address with destination IP address and source upper protocol port number with destination upper protocol port number. However, when `-ip_pair` or `-port_pair` is specified, this option performs checking according to that parameter setting.

`-pair_synchronized`: Checks for not switching source IP address and switching source IP address with destination IP address and source upper protocol port number with destination upper protocol port number (see Note later in this subsection). When you specify this option, set the IP address pair switch and the upper protocol port number pair switch to off (`-ip_pair_off, -port_pair_off`).

When specifies this parameter, define 6 (TCP) or 17 (UDP) to -protocol parameter. If -protocol is undefined or defined other than 6 (TCP) or 17 (UDP), this parameter becomes invalid.

Default: Off

Downloaded from www.Manualslib.com manuals search engine

Note: When using IP address pair switch, high-order protocol port No. pair switch, or IP address high-order protocol port No. synchronization switch, pay attention to the following:

(1) When using IP address pair switch for "-ip_pair": When using source IP address and destination IP address for range specification, set not to overlap the source IP address range and destination IP address range. If these ranges overlap, take either of the following actions:

Set pair switch to -ip_pair_off; -port_pair_off; -pair_synchronized.

Divide the definition of filter list information so as not to overlap the IP addresses.

(2) When using high-order protocol port No. pair switch for "-port_pair": When using source high-order protocol port No. and destination source high-order protocol port No. for range specification, set not to overlap the source high-order protocol port No. and destination source high-order protocol port No. range. If these ranges overlap, take either of the following actions:

Set pair switch to -ip_pair_off; -port_pair_off; -pair_synchronized.

Divide the definition of filter list information so as not to overlap the high-order protocol port.

(3) When using IP address pair switch, high-order protocol port No. pair switch, or IP address high-order protocol port No. synchronization switch by combining them, use them in the combination shown in Tables Table 1-60 and 1-61. The setting values of an upper protocol port number's pair switch and IP address upper protocol number's interlock pair switch are validated when 6(TCP) or 17(UDP) is defined in the upper protocol number. The setting values of an upper protocol port number's pair switch and IP address upper protocol number's interlock pair switch are invalidated when the upper protocol number is undefined or when numbers other than 6(TCP) or 17(UDP) are defined in the upper protocol number.

Downloaded from www.Manualslib.com manuals search engine

Table 1-60 Combination of Pair Switch

No.	Combination of Pair Switch			Setting	Processing
1	-Pair_synchronized_off	-port_pair_off	-ip_pair_off	Available	Checks the O‘ address and high-order protocol port No. by not switching source and destination.
2			-ip_pair	Available	The source and destination upper protocol port numbers are checked without being replaced. Checks the source IP address by both cases of switching/not switching source and destination.
3		-port_pair	-ip_pair_off	Available	Checks the source high-order protocol No. by both cases of switching/not switching source and destination. The source and destination IP addresses are checked without being replaced.
4			-ip_pair	Available (Default)	For the IP address and upper protocol port number, the source and destination are checked in both cases below. • When they are not replaced • When they are replaced
5	-pair_synchronized	-port_pair_off	-ip_pair_off	Available	For the IP address and upper protocol port number, the source and destination are checked in the cases below. • When both of them are not replaced • When both of them are replaced at the same time.
6			-ip_pair	Not available	—
7		-port_pair	-ip_pair_off	Not available	—
8			-ip_pair	Not available	—

Table 1-61 Combined Setting of Pair Switch and Possibility of Use

No.	Combined Setting of Pair Switch (Note)	Possibility of Use	Processing
1	-ip_pair_off	Possible	The source and destination IP addresses are checked without being replaced.
2	-ip_pair	Possible	For the IP address and upper protocol port number, the source and destination are checked in both cases below. • When they are not replaced • When they are replaced

Note: -port_pair_off/-port_pair and -pair_synchronized_off/-pair_synchronized switches are invalidated when the upper protocol number is undefined or when numbers other than 6(TCP) or 17(UDP) are defined in the upper protocol number.

Downloaded from www.Manualslib.com manuals search engine

{-ack_check_off | -ack_check}

Description: Specifies TCP one-way communication permission (ACK flag). The -ack_check_off option excludes the packet from filtering when its ACK flag is on. The -ack_check option filters the packet when its ACK flag is on.

Default: -ack_check_off

Range of value: None

{-syn_check_off | -syn_check}

Description: Specifies permission for establishing a virtual circuit (SYN flag). The -syn_check_off option excludes the packet from filtering when its SYN flag is on. The -syn_check option filters the packet when its SYN flag is on.

Default: -syn_check_off

Range of value: None

Note: Define the filtering according to the *GR2000 Configuration Settings (universal CLI)* manual when the IPv4 packets shown in the table below are filtered under the ACK/SYN flag conditions of a TCP header.
The filtering of the IPv4 packets shown in the table below that is performed under the ACK/SYN flag conditions of a TCP header is limited when IPv4 packets are used in a way except as described above. The IPv4 packets cannot be properly filtered even if "ack" and "syn" parameters are set to the filter flow information.

Table 1-62 Packet Type in which the Filtering Based on the Flag (ACK and SYN) Conditions of TCP Header Is Limited in Use

Packet Type	Limited Filtering Item
IPv4 packet generated by this router	• IPv4 packets do not match the filter list, to which "-ack_check" or "-syn_check" is set, in conditions. In other words, both ACK and SYN flags are searched for filtering as if packet 0 were input.
Packet applied to the conditions below among the IPv4 packets relayed by this router: (1) Packet with option (IP header)	The same as described above.
Packet applied to the conditions below among the IPv4 packets relayed by this router: (2) Packet requiring fragmentation (3) Packet requiring redirection (4) Packet in which ARP has not been solved	• The packets to be discarded are properly discarded when they conform to the filtering conditions. • The packets to be relayed do not match the filter list, to which "-ack_check" or "-syn_check" is set, in conditions when they conform to the filtering conditions. In other words, both ACK and SYN flags are searched for filtering as if packet 0 were input.

-icmp_type <No.>

Description: Specifies the ICMP type number in decimal

Default: Undefined

Range of value: 0–255

Downloaded from www.Manualslib.com manuals search engine

-icmp_code <No.>

Description: Specifies the ICMP code number in decimal.

Default: Undefined

Range of value: 0–255

-igmp_type <No.>

Description: Specifies the IGMP type number in decimal. When specifying this parameter, define 2 (IGMP) to -protocol. If -protocol is undefined or defined other than 2 (IGMP), this parameter becomes invalid.

Default: Undefined (Does not include IGMP type to the -filter condition.)

Range of value: 0–255

Table 1-63 IGMP Type Number

IGMP Type No. (h)	Input Value (Decimal)	Name
0x11	17	Membership Query
0x12	18	Version 1 Membership Report
0x13	19	DVMRP protocol
0x16	22	Version 2 Membership Report
0x17	23	Version 2 Leave Group
0x22	34	Version 3 Membership Report

-branch_index <No.>

Description: Specifies the connection branch index number (specified by the DLCI-group information or VC-group information) in decimal. When a packet that matches the filter condition is relayed, the DLCI/VC specified in the group is selected and transmitted. Select the filter list information that sets the connection branch index number as a transmitter's filter condition by means of -out (outbound) parameter of the filter-interface object.

Default: Undefined

Range of value: 0–7

-policy_routing <Interface Name> <IP Address>

Description: Enables the policy routing function by specifying the destination interface name (same as the line name set by the ip object) and the next hop IP address. The policy routing function causes the local device to relay a received packet to its destination if it matches the filter condition. Select the filter list information that sets the policy routing as a receiver's filter condition by means of –in (inbound) parameter of the filter-interface object.

Default: No policy routing

Range of value: Interface name: One of the line names set by the ip object.

Downloaded from www.Manualslib.com manuals search engine

Set the IP addresses below.
Class A: 1.0.0.1 to 126.255.255.254
Class B: 128.1.0.1 to 191.254.255.254
Class C: 192.0.1.1 to 233.255.254.254
IP address (127.0.0.0 to 127.255.255.255), and IP address of class D (224.0.0.0 to 239.255.255.255)
A broadcast address (in which net ID or host ID is all "1" or all "0" in binary) cannot be set.

`-policy_routing_group <policy-Group-Name>`

Description: Specifies policy group name defined by policy-group information. When relaying packet that matches the filter condition, sends the packet to the most priority path in the output destination registered in policy group specified by this option. Policy group as the filter condition of receiving side by specifying -in (Inbound) when setting filter interface information. (See Subsection 1.1.13 filter interface for details.)

Default: Undefined (Invalidates policy routing function.)

Range of value: Policy group name specified by policy-group information.

`-replace_tos <New Tos>`

Description: Enables the TOS rewriting function and Diff-serv DS field rewriting function by specifying a new TOS in decimal. In the latter case, the high-order 6 bits of the new TOS are used and the low-order two bits are ignored. Table 1-64 summarizes how this option works. See Subsection 1.2.7 for further information.

Default: No TOS rewriting (TOS-QoS conversion table is retrieved with the TOS of the received packet.)

Range of value: 0–255

Table 1-64 Replace_TOS Field Rewriting

Set Content	IP Header TOS Field Rewriting	TOS-QoS Conversion Table Retrieval*
Replace_tos<New Tos>	Rewrite packet TOS with specified TOS	Retrieve TOS after rewriting

Example

1. Set the condition to permit (relay) FTP from the transmit source in filter list number 1 to the destination with these options:
   - Operation type: - `forward` (relay)
   - Upper rank protocol number: 6 (TCP)
   - Transmit source IP address: 123.123.1.1-123.123.1.123
   - Destination IP address: 123.123.2.1

   Transmit source high-rank protocol port number: 20-21(`ftp_data,ftp`)

   Method of checking synchronization of IP address and upper rank protocol port number: `-pair_synchronized` (switch check done at same time)

Downloaded from www.Manualslib.com manuals search engine

To specify -pair_synchronized, specify the method of checking the IP address as ip_pair_off and the method of checking the upper-rank protocol port number as port_pair_off.

```
(config)#filter -yes
(config)#filter-list 1 -forward -protocol 6 -ip_source
123.123.1.1 -123.123.1.123 \
-ip_destination 123.123.2.1 -port_source 20 -21
-pair_synchronized –ip_pair_off \
-port_pair_off
(config)#show filter-list
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
(config)#
```

2. Change the destination IP address of filter list number 1 from 123.123.2.1 to 123.123.2.1-123.123.2.123.

```
(config)#filter-list 1 –ip_destination 123.123.2.1
–123.123.2.123
(config)#show filter-list
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1-123.123.2.123;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
filter_list 2 {
forward;
protocol 1;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
icmp_type 8;
icmp_code 0;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Delete parameters of filter list information:

```
(config)#show filter-list 1
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1-123.123.2.123;
port_pair_off;
port_source 20-21;
pair_synchronized;
};
(config)#delete filter-list 1 -ip_source
(config)#show filter-list 1
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_destination 123.123.2.1-123.123.2.123;
port_pair_off;
port_source 20-21;
pair_synchronized;
};
(config)#
```

4. Show all filter list information:

```
(config)#show filter-list
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1-123.123.2.123;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
filter_list 2 {
forward;
protocol 1;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
icmp_type 8;
};
filter_list 3 {
forward;
protocol 2;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
igmp_type 0;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

5. Show filter list number 2 information:

```
(config)#show filter-list 2
filter_list 2 {
forward;
protocol 1;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
icmp_type 8;
};
(config)#
```

6. Delete filter list number 2:

```
(config)#show filter-list
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1-123.123.2.123;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
filter_list 2 {
forward;
protocol 1;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1-123.123.2.123;
icmp_type 8;
icmp_code 0;
};
filter_list 3 {
forward;
protocol 2;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
igmp_type 0;
};
(config)#delete filter-list 2
(config)#show filter-list
filter_list 1 {
forward;
protocol 6;
ip_pair_off;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1-123.123.2.123;
port_pair_off;
port_source 20–21;
pair_synchronized;
};
filter_list 3 {
forward;
protocol 2;
ip_pair;
ip_source 123.123.1.1-123.123.1.123;
ip_destination 123.123.2.1;
igmp_type 0;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

7. Display of blank entry number
   - Display of all blank entry numbers

```
(config)# show ffilter-list free
Free number: 5,7,15-1024
(config)#
```

   - Display of first blank entry number

```
(config)# show filter-list free min_no
Free number: 5
(config)#
```

Related Configuration Object

filter
filter-group
filter-interface
qos-tos-map
dlci_group
vc-group
policy-group

Precautions

1. A maximum of 1024 filter list conditions can be created with each device.
2. Filter list being used by filter group cannot be deleted.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.1.12 *filter-group* (Information on Filter Group of Old BSD UNIX-Based Command System)

Function

Object for creation, modification, deletion, and display of the filter group information. Register in the order of judging the filter conditions defined by the filter list. A maximum of 256 filter groups can be created, and the total filter conditions of all groups must be 1024 or less.

Input Format

To create the filter group information:

```
[set]filter-group<Filter-Group-Name><Filter List No.>
```

To modify the filter group information:

```
[set]filter-group<Filter-Group-Name><Filter List No.>
```


Downloaded from www.Manualslib.com manuals search engine

To delete the filter group information:

```
delete filter-group<Filter-Group-Name>[<Filter List No.>]
```

To show the filter group information:

```
show filter-group[<Filter-Group-Name>]
```

To insert the filter group information:

```
insert filter-group<Filter-Group-Name><Insert Position Filter List No.>
<Filter List No.>
```

Parameters

`<Filter-Group-Name>`

Description: Specifies the filter group name up to 14 characters.

Default: Undefined. Mandatory input except for display. When omitted, all specified filter groups are deleted or displayed.

`<Filter List No.>`

Description: Specifies the filter list number. Set the filter list information before entering this command.

Default: Undefined. Mandatory input except for deletion and display. When omitted, all specified filter groups are deleted or displayed.

Range of value: 1–1024

`<Insert Position Filter List No.>`

Description: Specifies the filter list number to be inserted. It is inserted one position before the specified filter list number.

Default: Undefined (mandatory input)

Range of value: 1–1024

Examples

1. Set filter list number 3 in filter group name ip1:

```
(config)#filter -yes
(config)#filter-list 3
(config)#filter-list 9
(config)#filter-list 18
(config)#filter-group ip1 3
(config)#show filter-group ip1
filter_group ip1 {
filter_list 3;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Add filter list number 18 at the end of filter group name ip1:

```
(config)#show filter-group ip1
filter_group ip1 {
filter_list 3;
};
(config)#filter-group ip1 18
(config)#show filter-group ip1
filter_group ip1 {
filter_list 3;
filter_list 18;
};
(config)#
```

3. Show the contents of all filter groups:

```
(config)#show filter-group
filter_group ip1{
filter_list 3;
filter_list 18;
};
filter_group ip2{
filter_list 2;
filter_list 3;
filter_list 4;
filter_list 10;
};
(config)#
```

4. Show the contents of filter group name ip1:

```
(config)#show filter-group ip1
filter_group ip1{
filter_list 3;
filter_list 18;
};
(config)#
```

5. Insert the configuration information
   Insert filter list number 9 in front of filter list number 18 of filter group name ip1.

```
(config)#show filter-group ip1
       filter_group ip1 {
                filter_list 3;
                filter_list 18;
       };
(config)#insert filter-group ip1 18 9
(config)#show filter-group ip1
       filter_group ip1 {
                filter_list 3;
                filter_list 9;
                filter_list 18;
       };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Delete filter list number 9 of filter group name ip1:

```
(config)#show filter-group ip1
filter_group ip1 {
filter_list 3;
filter_list 9;
filter_list 18;
};
(config)#delete filter-group ip1 9
(config)#show filter-group ip1
filter_group ip1 {
filter_list 3;
filter_list 18;
};
(config)#
```

7. Delete filter group name ip1:

```
(config)#show filter-group ip1
filter_group ip1 {
filter_list 3;
filter_list 18;
};
filter_group ip2 {
filter_list 1;
};
(config)#delete filter-group ip1
(config)#show filter-group ip1
filter_group ip2 {
filter_list 1;
};
(config)#
```

Related Configuration Objects

`filter`

`filter-list`

`filter-interface`

Precautions

1. Set the filter list before setting the filter group.
2. The filter is executed in the order of the filter list numbers specified in the filter group (order of display when `show filter-group` is executed.)
3. A maximum of 256 filter groups can be created, and the total filter conditions of all groups must be 1024 or less.
4. The filter list number of the conditions under which packets are relayed and the filter list number of the conditions under which all packets are discarded are sequentially registered when only a specific packet is relayed. All packets are relayed when the filter conditions under which all packets are discarded are not registered.
5. When forwarding packets other than the specific ones to be discarded, register only the filter list number of the discard condition.
6. More than one of the same filter list number cannot be registered in one filter group.
7. A filter group being used in the filter interface cannot be deleted.

Downloaded from www.Manualslib.com manuals search engine

8. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.1.13 *filter-interface* (Information on Filter Interface of Old BSD UNIX-Based Command System)

Function

Object for creation, modification, deletion, and display of the filter interface information. The filter group is allocated to the interface defined by the IP or IP-address information. When the filter interface is set, the filter for the receive packet or the transmit packet in the relevant interface is judged. A maximum of 512 filter interfaces per RP can be created.

Input Format

To create the filter interface information:

```
[set] filter-interface { <Line Name> | <DLCI Name> | <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name> } { -in | -out } -filter_group
<Filter Group Name>
```

To modify the filter interface information:

```
[set] filter-interface { <Line Name> | <DLCI Name> | <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name> } { -in | -out } -filter_group
<Filter Group Name>
```

To delete the filter interface information:

```
delete filter-interface { <Line Name> | <DLCI Name> | <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name> } { -in | -out }
```

To show the filter interface information:

```
show filter-interface [{ <Line Name> | <DLCI Name> | <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name> }]
```

Parameter

`{ <Line Name> | <DLCI Name> | <VC Name> | <Group Name> | <Timeslot Name> | <Peer Name> }`

Description: Specifies the target interface name predefined by the ip or ip-address object.

Default: Undefined. Mandatory input other than for display. When omitted, all filter interface information is displayed.

`{-in | -out}`

Description: Specifies inbound or outbound. Either one or both of inbound/outbound can be set at the same time.

-in: Inbound (specify when filtering on receive side of frame)

Downloaded from www.Manualslib.com manuals search engine

-out: Outbound (specify when filtering on transmit side of frame)

Default: Undefined

`-filter_group <Filter-Group-Name>`

Description: Specifies the filter group name. Set the filter group information before entering this command.

Default: Undefined

Example

1. Set filter group name `ip1` in inbound of interface name `ether1`:

```
(config)#line ether1 ethernet 0/0
(config)#ip ether1 170.10.10.10/24
(config)#filter -yes
(config)#filter-list 1
(config)#filter-group ip1 1
(config)#filter-interface ether1 in –filter_group ip1
(config)#show filter-interface ether1
filter_interface ether1 in filter_group ip1;
config
```

2. Set filter group name `ip1` in inbound and filter group name `ip2` in outbound of interface name `ether1`:

```
(config)#line ether1 ethernet 0/0
(config)#ip ether1 170.10.10.10/24
(config)#filter -yes
(config)#filter-list 1
(config)#filter-group ip1 1
(config)#filter-interface ether1 -in –filter_group ip1
(config)#filter-interface ether1 -out –filter_group ip2
(config)#show filter-interface ether1
filter_interface ether1 in filter_group ip1;
filter_interface ether1 out filter_group ip2;
(config)#
```

3. Change the filter group name set in inbound of interface name `ether1` from `ip1` to `ip2`:

```
(config)#show filter-interface ether1
filter_interface ether1 in filter_group ip1;
filter_interface ether1 out filter_group ip2;
(config)#filter-interface ether1 -in –filter_group ip2
(config)#show filter-interface ether1
filter_interface ether1 in filter_group ip2;
filter_interface ether1 out filter_group ip2;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Show all the contents:

```
(config)#show filter-interface
filter_interface ether1 in filter_group ip2;
filter_interface ether1 out filter_group ip2;
filter_interface ether2 in filter_group ip1;
filter_interface ether3 out filter_group ip3;
(config)#
```

5. Show the contents of interface name ether1:

```
(config)#show filter-interface ether1
filter_interface ether1 in filter_group ip2;
filter_interface ether1 out filter_group ip2;
(config)#
```

6. Delete the definition of inbound of interface name ether1:

```
(config)#show filter-interface ether
filter_interface ether1 in filter_group ip2;
filter_interface ether1 out filter_group ip2;
(config)#delete filter-interface ether1 in
(config)#show filter-interface ether1
filter_interface ether1 out -filter_group ip2;
(config)#
```

Related Configuration Object

- filter
- filter-list
- filter-group
- ip
- ip-address

Precaution

1. A maximum of 512 entries of filter interface information per RP can be created (maximum interface 256, inbound/outbound per interface).
2. Set filter group information, IP information, and IP-address information before executing this command.
3. More than one filter group cannot be specified for inbound/outbound on one interface.
4. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

1.2 Quality of Service (QoS) Objects

This section describes the parameters and configuration commands that define QoS. QoS control enables transmission of IP packets by priority, with highest-priority packets transmitted first. The following is a brief description of each component of the overall QoS control mechanism, with associated configuration commands displayed for each block.

1. QoS enable/disable

   QoS information (qos) specifies whether QoS is functional or nonfunctional.

   → 1.2.1 qos (QoS information)

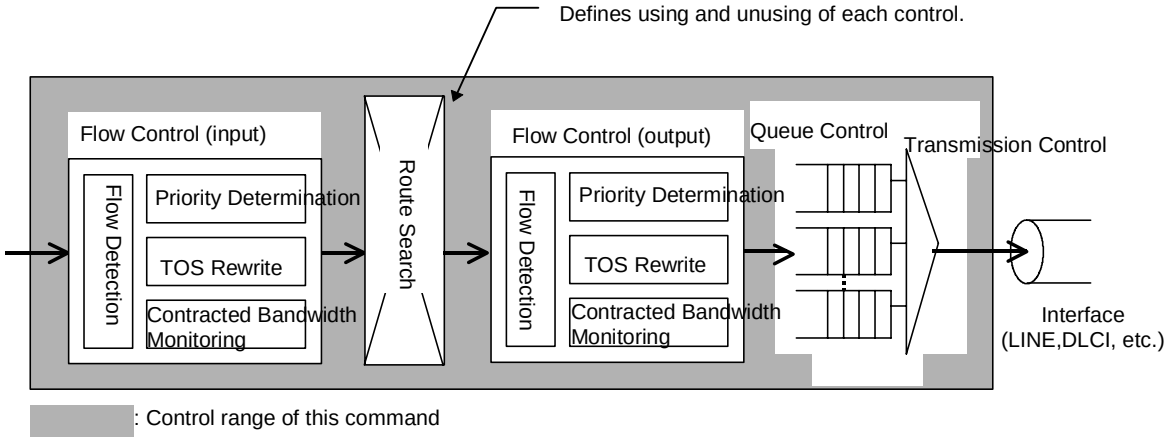


Figure 1-4 Control Range of QoS Information

2. Transmission control

   Transmission control determines the output queue mode, thereby controlling the precedence of packets on the interface output queue. There are three queue modes: priority, round-robin, and bandwidth. The QoS queue attribute command (qos-queue-list) generates interface output queue lists; the QoS interface command (qos-interface) applies the queue list for each interface.

   → 1.2.2 qos-queue-list

   → 1.2.3 qos-interface

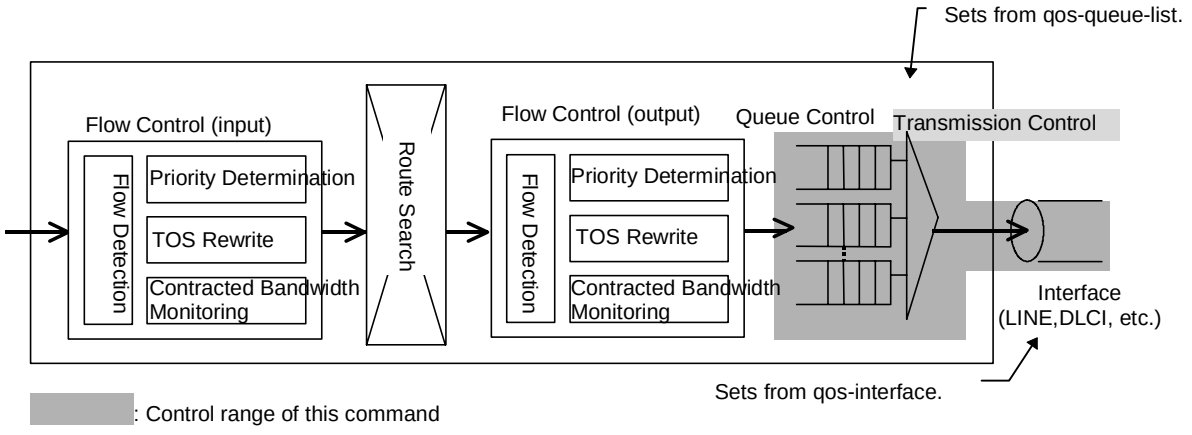


Figure 1-5 Range of QoS Attribute and Qos Interface Control

Downloaded from www.Manualslib.com manuals search engine

3. Queue control

When there is a backlog on the output queue, packets remaining on the queue are transmitted or discarded depending on priority. The QoS discard mode command (qos-discard-mode) sets queue size and enables queuing by priority class.

→ 1.2.4 qos-discard-mode

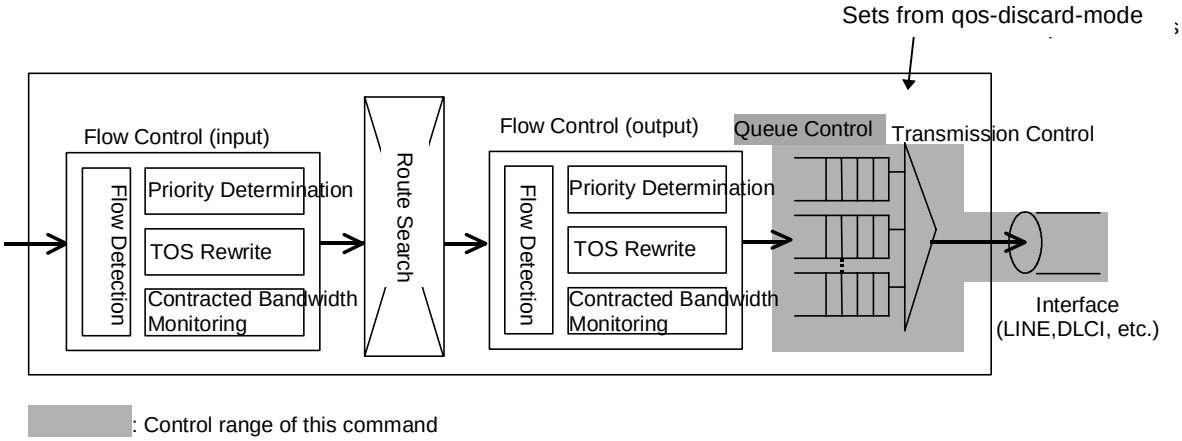


Figure 1-6 Range of QoS Discard Mode Control

4. Flow control

The flow-control function identifies incoming IP packets by their flow-control settings, determines priority, rewrites TOS, and manages reserved bandwidths. The flow control includes two input form for configuration definition. Features of each input form are shown in Table 1-65.

Table 1-65 Features of Constituting Definition of Filter Flow Information by Input Form

Item	Constituting Definition Inputting Form	
	qos-ip-list, qos-ip-list-group, qos-ip	***flow filter***
Number of entry(*1)	1024 entry/device	10000 entry/device 2000 entry/RP
Inputting form	Input three commands to define one list. Effective in defining the same flow control in multiple number of input/output interfaces.	Input one command to define one list. Effective in inputting a number of entries.
Function use, and unused unit	Device unit	Device unit, and input/output interface unit
Operation command Indication unit for qos ip flow.	Device unit and list unit	Device unit and input/output interface unit
Vacant entry indication	Supported.	Unsupported.
**1: Total value with entries of filters.*		

For the configuration definition flow qos, please refer to Subsection 1.1.7 "flow qos". The configuration definitions qos-ip-list, qos-list-group, and qos-ip are described below.

The QoS IP list (qos-ip-list) command generates lists defining flow detection conditions and the various types of flow control active in flow detection. The QoS IP list group (qos-ip-list-group) command assigns a decision order to lists, allowing

Downloaded from www.Manualslib.com manuals search engine

information to be collated into a single group. Finally, IP QoS (qos-ip) applies the group used on each interface.

→ 1.2.5 qos-ip-list

→ 1.2.6 qos-ip-list-group

→ 1.2.8 qos-ip

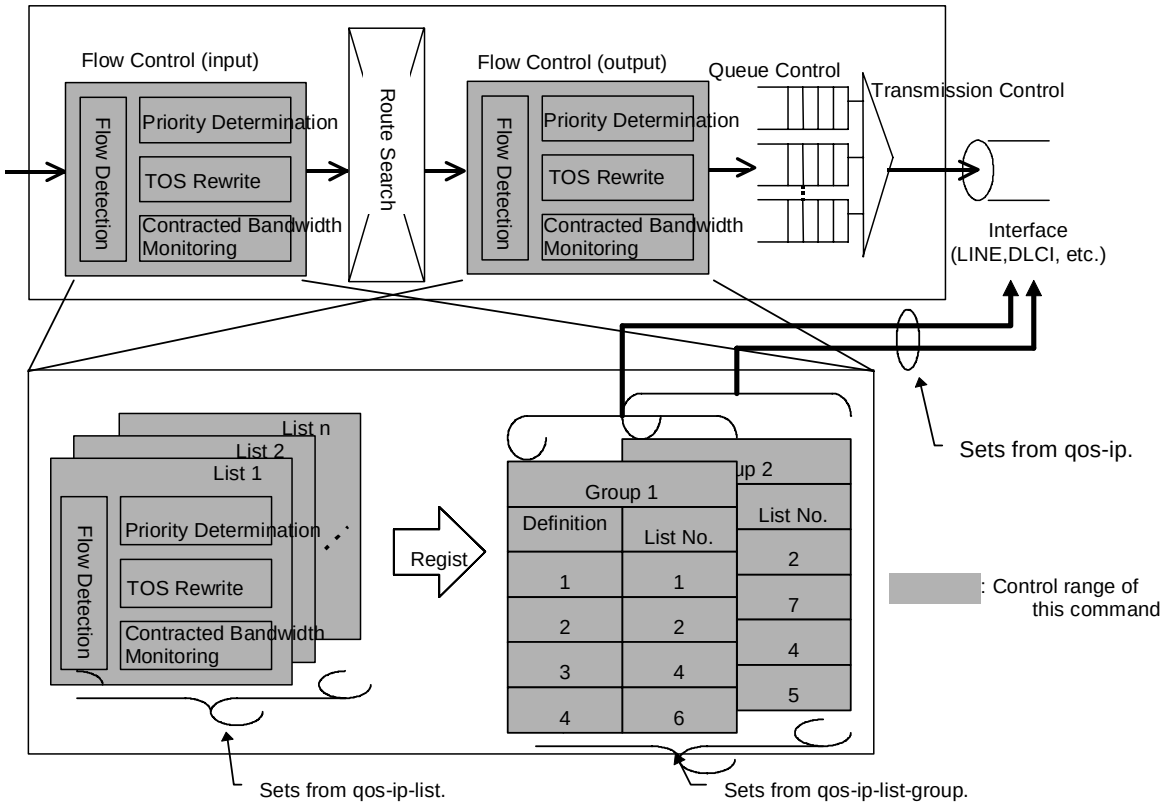


Figure 1-7 Range of QoS IP Frame Condition Information, QoS IP Frame Condition Group Information, and IP QoS Information Control

5. TOS-QoS conversion table for priority determination

This table determines the priority of incoming IP packets detected by flow control using either the packets' TOS values or rewritten TOS values. The TOS-QoS conversion table (qos-tos-map) command determines priority for each TOS field precedence.

Downloaded from www.Manualslib.com manuals search engine

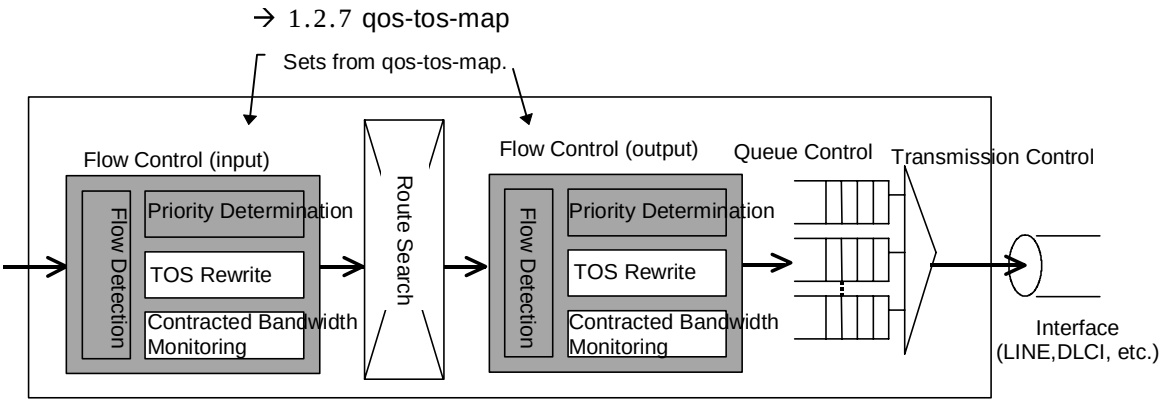


Figure 1-8 Range of TOS-QoS Conversion Table Information Control

6. Non-IP protocol QoS control

   Non-IP protocol (IPX, Bridge, HDLC, etc.) QoS control is set using three commands: IPX QoS (qos-ipx), bridge QoS (qos-bridge), and HDLC QoS (qos-hdlc). These define QoS control for IPX, Bridge, and HDLC protocols, respectively.

   → 1.2.9 qos-ipx

   → 1.2.10 qos-bridge

   → 1.2.11 qos-hdlc

1.2.1 *qos*

This command sets the use and disuse of flow control. The setting of use and disuse is enabled when the flow control is set using the old, BSD UNIX-based command system (qos-ip-hst, quos-ip-hst-group, or qos-ip). The setting of use and disuse in this command is disabled when the flow control is set using a flow command. Set the use and disuse using a flow command when setting the flow control using a flow command.

Input Format

Setting information

```
[set] qos {-no | -yes} [-cops][-wan_length_mode {short | long}]
```

Modifying information

```
[set] qos {-no | -yes} [-cops][-wan_length_mode {short | long}]
```

Deleting information

```
delete qos
```

Displaying information

```
show qos
```

Parameters

```
{-no | -yes}
```

Description: enable/disable flow control

-no: disable

Downloaded from www.Manualslib.com manuals search engine

-yes: enable

Default: no

[-cops]

Description: This parameter uses all interfaces by a COPS function.

Default: None (All interfaces are not used by a COPS function.)

-wan_length_mode { short | long}

Description: Designates in the device unit the length of a hardware queue that is used in frame transmission to WAN lines smaller than 6 M bit/s (serial, BRI, PRI, J2, BRIISDN, PRIISDN, T1, ED) and the E3 multiplex line.

Short: Hardware queue length gives the transmission delay time higher priority.

Long: Hardware queue length gives performance higher priority.

Default: Short.

Example

1. Setting QoS parameters

   To enable flow control:

```
(config)#qos yes
(config)#show qos
qos yes;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Modifying Parameters:

   To disable flow control (invalidates previous flow control):

```
(config)#show qos
qos yes {
qos_queue_list queueA priority;
qos_interface office1 queueA;
qos_discard_mode nif 0 discard_mode 3;
qos_ip_list 1 {
ip_destination 123.123.2.1;
replace_tos 240 upc 1000000 upc_penalty drop;
};
qos-ip-list-group ip1 {
ip_list 1;
};
qos-ip office1 in ip_list_group ip1;
}
(config)# qos -no
(config)# show qos
qos no {
qos_queue_list queueA priority;
qos_interface office1 queueA;
qos_discard_mode nif 0 discard_mode 3;
qos_ip_list 1 {
ip_destination 123.123.2.1;
replace_tos 240 upc 1000000 upc_penalty drop;
};
qos-ip-list-group ip1 {
ip_list 1;
};
qos-ip office1 in ip_list_group ip1;
}
(config)#
```

3. Deleting parameters:

   To delete flow control settings (parameters cannot be deleted when QoS configurations other than QoS information have been specified):

```
(config)#show qos
qos yes;
(config)#delete qos
(config)#
```

4. Displaying QoS settings:

   To display all configuration for the QoS function:

```
(config)#show qos
qos yes {
qos_queue_list queueA priority;
qos_interface office1 queueA;
qos_discard_mode nif 0 discard_mode 3;
qos_ip_list 1 {
ip_destination 123.123.2.1;
replace_tos 240 upc 1000000 upc_penalty drop;
};
qos-ip-list-group ip1 {
ip_list 1;
};
qos-ip office1 in ip_list_group ip1;
}
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related commands

qos-queue-list
qos-interface
qos-discard-mode
qos-ip-list
qos-ip-list-group
qos-tos-map
qos-ip
qos-ipx
qos-bridge
qos-hdlc
cops

Precautions

1. Before invoking any of the related commands above, set the proper command configuration. Once the configuration has been set for a given command, the command may be entered continuously, unless and until the QoS settings are deleted.
2. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
3. The cops parameter of this command cannot be deleted when COPS configuration definition is set.
4. The cops parameter of this command cannot be set when qos-interface (QoS interface information) is set.
5. The cops parameter of this command cannot be set when qos-queue-list (QoS queue attribute) is set.
6. The following table illustrates the relationship between QoS setting and QoS command effectiveness and ineffectiveness.

Table 1-66 Relationship Between QoS Command Effectiveness and Ineffectiveness

Command Name	Command Explanation	QoS Setting	
		qos yes	***qos no***
flow qos	Flow QoS information	(*1)	
qos-queue-list	QoS queue attribute	√	√
qos-interface	QoS interface information	√	√
qos-discard-mode	QoS abolishment information	√	√
qos-ip-list	QoS IP frame condition information for the old BSD UNIX-based command system	√	–
qos-ip-list-group	QoS IP frame condition group information for the old BSD UNIX-based command system	√	–
qos-ip	IP QoS information for the old BSD UNIX-based command system	√	–

√: Effective, -: Ineffective
**1: Depends on the* flow *command's effectiveness/ineffectiveness*

Downloaded from www.Manualslib.com manuals search engine

Table 1-66 Relationship Between QoS Command Effectiveness and Ineffectiveness

Command Name	Command Explanation	QoS Setting	
		qos yes	*qos no*
qos-tos-map	TOS-QoS conversion table information	√	√
qos-ipx	IPX QoS information	√	√
qos-bridge	Bridge QoS information	√	√
qos-hdlc-passthrough	HDLC QoS information	√	√

√: Effective, -: Ineffective
**1: Depends on the* flow *command's effectiveness/ineffectiveness*

1.2.2 *qos-queue-list*

This command assigns a name to the QoS queue list, defines the QoS mode (priority, round-robin, or bandwidth), and allocates bandwidth when QoS mode is set for bandwidth. A maximum of 256 entries may be created for each RP.

Input Format

Setting/modifying information

```
[set] qos-queue-list <Queue List Name>
     [{-priority | -round_robin | -bandwidth | -equal_bandwidth
     [-queue_number <Queue Number>] | -bandwidth_kbps |
     -bandwidth_traffic <kbps>}]
     [{[-queue1_bandwidth <Rate>][-queue2_bandwidth <Rate>]
     [-queue3_bandwidth <Rate>][-queue4_bandwidth <Rate>]
     [-queue5_bandwidth <Rate>][-queue6_bandwidth <Rate>]
     [-queue7_bandwidth <Rate>][-queue8_bandwidth <Rate>]
     [-queue9_bandwidth <Rate>][-queue10_bandwidth <Rate>]
     [-queue11_bandwidth <Rate>][-queue12_bandwidth <Rate>]
     [-queue13_bandwidth <Rate>][-queue14_bandwidth <Rate>]
     [-queue15_bandwidth <Rate>][-queue16_bandwidth <Rate>]}]
[{-max_queue_number_4 |-max_queue_number_8
| -max_queue_number_16| -max_queue_number_32
| -max_queue_number_64| -max_queue_number_250
| -max_queue_number_1000}]
[ -queue <Queue No.>, <Queue No.> - <Queue No.>, º <min rate (kbps)>]
[-traffic <Queue No.> -constant  -peak_rate <kbps>]
[-traffic <Queue No.> -guarantee  -min_rate <kbps>
[-peak_rate <kbps>] [-weight <Rate>]]
```

Deleting information

```
delete qos-queue-list <Queue List Name>
```

Displaying information

```
show qos-queue-list [<Queue List Name>]
```


Downloaded from www.Manualslib.com manuals search engine

Table 1-67 shows parameters to be set per queue mode.

Table 1-67 Parameters To Be Set Per Queue Mode

Parameter	Queue Mode					
	Priority Control	Round-Robin	Minimum Bandwidth Guarantee	Equal Minimum Bandwidth Guarantee	Minimum Bandwidth Guarantee (kbit/s)	Bandwidth Control (traffic)
<Queue List Name>	X	X	X	X		X
-priority	X					
-round_robin		X				
-bandwidth			X			
-equal_bandwidth				X		
-bandwidth_kbps					X	
-bandwidth_traffic						X
-queue_number <Queue Number>				X		
-queueX_bandwidth (X: 1-16)			X			
[{-max_queue_number_4[ROUTE-OS 6B] | -max_queue_number_8 | -max_queue_number_16| -max_queue_number_32| -max_queue_number_64 [ROUTE-OS6B] |-max_queue_number_250| -max_queue_number_1000}]					X	
[-queue <Queue No.>, <Queue No.>-<Queue No.>, ... <min rate (kbps)>]					X	
-traffic <Queue No.> -constant -peak_rate <kbps>						X
-traffic <Queue No.> -guarantee -min_rate <kbps> [-peak_rate <kbps>] [-weight <Rate>]						X
X: Required						

Parameters

`<Queue List Name>`

Description: Specifies the queue list name

Default: No default; only the displayed value is supported.

Range of value: Character strings must begin with an alphabetic character and contain no more than 14 characters.

`{ -priority | -round_robin | -bandwidth | -equal_bandwidth | -bandwidth_kbps | -bandwidth_traffic <kbps>}`

Description: Sets the queue mode

`-priority`: output priority control

`-round_robin`: round-robin scheduling

`-bandwidth`: minimum bandwidth guarantee

Downloaded from www.Manualslib.com manuals search engine

-equal_bandwidth: equal minimum bandwidth guarantee

-bandwidth_kbps: minimum bandwidth guarantee (kbps)

-bandwidth_traffic<kbit/s>: bandwidth control (traffic) <maximum transmission band of a line>.

Default: None

Range of value:

The setting range of a value differs for each line type.

Table 1-68 shows the range in which the maximum transmission band of a line can be set.

Default: priority

Table 1-68 Maximum Range of Send Bandwidth

RP Type	NIF Type	Line type	Range (*1) (*2)			
			4 Number of Queues	8 Number of Queues	32 Number of Queues	64 Number of Queues(*3)
RP-A1,RP-D, RP-D6, RP-DV	NE100-8TB	10BASE-T full-duplex	--	1536 -100000	--	--
		100BASE-T full-duplex	--	1536 - 1000000	--	--
	NE1G-1SB	1000BASE-SX	--	1536 - 7000000	6144 - 7000000	--
	NE1G-1LB	1000BASE-LX	--	1536 - 7000000	6144 - 7000000	--
	NE1G-1LHBA	1000BASE-LH	--	1536 - 7000000	6144 - 7000000	--
RP-C,RP-C6, RP-CV	NE1G-4C	1000BASE-SX 1000BASE-LX 1000BASE-LH	--	1536 - 7000000	6144 - 7000000	--
GR2000-1B GR2000-2B	Ethernet containing GR2000-1B and GR2000-2B NEB100-4TB NEB1G-1B	10BASE-T full-duplex	320 - 10000	640 - 10000	--	5120 - 10000
		100BASE-TX full-duplex	320 - 10000	640 - 10000	--	5120 - 10000
		1000BASE-SX 1000BASE-LX 1000BASE-LH	320 - 590000	640 - 590000	--	5120 - 590000
GR2000-BH	NEBH1G-4C	1000BASE-SX 1000BASE-LX 1000BASE-LH	--	1536 - 1000000	6144 - 1000000	--

**1: The maximum transmission band of the line can be set in 1 kbit/s units.*
**2: The router operates based on the output priority control when the value out of the range that can be set in the maximum transmission band of a line is set. If the maximum queue number has not been specified or if an ineffective value has been set, the number is automatically set at 8 (4 in the case of Ethernet containing GR2000-1B and GR2000-2B).*
**3: the maximum queue number can be set at 64 only when set to one line (Line number zero). The queue mode that can be used for each media type is as shown in the table below.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-69 Media Type and Available Queue Mode

Media and Layer 2 Protocol	NIF	Queue Control			Send Control					
		Unit for Holding Queue	Number of Queues	Queuing Priority Level	Output Priority Control	Minimum Bandwidth Guarantee	Round-robin	Uniform minimum band guarantee	Minimum Bandwidth Guarantee (specified in kbps)	Bandwidth control (specified in traffic)
Ethernet	NE100-8T NE100-8TA	Line	8	4	√	-- (*1)	√	-- (*1)	-- (*1)	-- (*1)
	Ethernet containing GR2000-2S NE100-4F NE100-4FS NE100-4FS4	Line	8	4	√	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)
Ethernet 10BASE-T half-duplex 100BASE-TX half-duplex	NE100-8TB	Line	8	4	√	-- (*5)	√	-- (*1)	-- (*1)	-- (*5)
	Ethernet containing GR2000-1B and GR2000-2B NEB100-4TB	Line	4	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)
		Line	8	4	√	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)
		Line	64	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)
Ethernet 10BASE-T ful-duplex 100BASE-TX full-duplex	NE100-8TB	Line	8	4	√	√	√	-- (*1)	-- (*1)	√ (*5)
	Ethernet containing GR2000-1B and GR2000-2B NEB100-4TB	Line	4	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√ (*5)
		Line	8	4	√	√	-- (*1)	-- (*1)	-- (*1)	√ (*5)
		Line	64	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√ (*5)
Gigabit Ethernet	NE1G-1S NE1G-1SA NE1G-1L NE1G-1LA NE1G-1LHA NE1G-1LHA8	Line	8	4	√	-- (*1)	√	-- (*1)	-- (*1)	-- (*1)
Gigabit Ethernet	NE1G-1SB NE1G-1LB NE1G-1LHBA NE1G-4C NEBH1G-4C	Line	8	4	√	√	√	-- (*1)	-- (*1)	√
			32	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√
	NEB1G-1B	Line	4	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√
			8	4	√	√	-- (*1)	-- (*1)	-- (*1)	√
			64	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√
Low speed WAN (to 6M) PPP	(*4)	Line	8	4	√	√	√	-- (*1)	√ (*3)	-- (*1)
			16	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√ (*3)	-- (*1)
			32	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√ (*3)	-- (*1)
			250	4	-- (*1)	-- (*1)	-- (*1)	-- (*1)	√ (*3)	-- (*1)
			1000	2	-- (*1)	-- (*1)	√	-- (*1)	√ (*3)	-- (*1)
High speed WAN (from 150M) PPP	(*4)	Line	8	4	√	√	√	-- (*1)	-- (*1)	-- (*1)

Downloaded from www.Manualslib.com manuals search engine

Table 1-69 Media Type and Available Queue Mode (continued)

Media and Layer 2 Protocol	NIF	Queue Control			Send Control					
		Unit for Holding Queue	Number of Queues	Queuing Priority Level	Output Priority Control	Minimum Bandwidth Guarantee	Round-robin	Uniform minimum band guarantee	Minimum Bandwidth Guarantee (specified in kbps)	Bandwidth control (specified in traffic)
Low speed WAN (to 6M) Frame Relay	(*4)	DLCI	8	4	√	√	√	√	-- (*1)	-- (*1)
			16	4	-- (*1)	√	-- (*1)	√	-- (*1)	-- (*1)
			32	4	-- (*1)	-- (*1)	-- (*1)	√	-- (*1)	-- (*1)
ISDN	(*4)	Peer	8	4	√	√	√	-- (*1)	-- (*1)	-- (*1)
ATM	(*4)	--	--	--	-- (*2)	-- (*2)	-- (*2)	-- (*2)	-- (*2)	-- (*2)

√: Supported, —: Not supported.
**1: Does not check configurations. Will operate system on the default value (priority mode).*
**2: Runs ATM QoS. The transmission control is performed by the traffic types of CBR, VBR, ABR, and UBR.*
**3: When bod option is specified to PPP information or when IPX routing interface or bridge interface is specified to PPP's interface, processed by default (priority) value. If the maximum queue number has not been set or if an ineffective value has been set, the number is automatically set at 8.*
**4: This NIF supports the functions described in the media and layer 2 protocol item.*
**5: In the minimum band guarantee and band control (traffic designation), the router does not operate in the specified band when the full-duplex setting of 10BASE-T/100BASE-TX is changed to half-duplex setting (including automatic negotiation).*

Precautions

- When the operating configurations are modified, interfaces using the modified list will restart.

`-queuen_bandwidth <Rate> (n is a number from 1-16)`

This setting is supported only in the -bandwidth queue mode; it is invalid in -priority or -round_robin mode. Bandwidth allocation is determined by the line rate; set this as a percentage figure. Limit the value for total bandwidth to 100 or less and indicate at least one queue within the -queue1_bandwidth-queue8_bandwidth setting. Enter a value of 1 or greater in -queue8_bandwidth at all times because RIP, ARP, and other frames implement queueing at queue8. If a packet for control is not allotted to the transmitting queue band, the packet for control at congestion of output lines may not be transmitted from this device, making the communication impossible due to breakage of the session. Table 1-70 shows categories of the control packets produced in this device.

Downloaded from www.Manualslib.com manuals search engine

Table 1-70 Categories of the Control Packets Outputted by Queue 8 or 16

Item No.	Control Packet Category Influence if Not Transmitted.
PPP-LCP control packet	Monitors link quality by using echo under the link setting condition. If the echo does not pass through, line quality NG may be detected erroneously.
PPP-NCP control packet	If the control packet negotiating execution of the high-order protocols (IP/IPX/Bridge/MPLS) does not pass through, no response from the counterpart station may be detected erroneously.
MPLS-LDP Hello packet	Possibility exists that the LSP session may be cut off.
MPLS-LDP KeepAlive packet	Possibility exists that the LSP session may be cut off.
ARP request/ response frame	Possibility exists that the communication becomes impossible because ARP cannot be solved.
RIP packet	Possibility exists that the communication becomes impossible because the route information is not distributed.
OSPF packet	Possibility exists that the communication becomes impossible because the route information is not distributed.
BGP packet	Possibility exists that the communication becomes impossible because the route information is not distributed.
TGMP packet	Possibility exists that the communication becomes impossible because the multicast information is not distributed.
PIM packet	Possibility exists that the communication becomes impossible because the multicast information is not distributed.

In addition, in case of WAN line, errors of several percent to 20% may occur because of the communication band (communication speed for the case of PPP, the minimum rate assurance value for the case of frame relay (-min_access_rate)) and the transmission packet length. The error grows if the smaller the communication band, and the longer the transmission packet.
The minimum bandwidth that can be specified is 1050 kbit/s when the line used is Ethernet. Therefore, set 0% or 11% or more when the line speed of the line used is 10 Mbit/s. Set 0% or 2% or more when it is 100 Mbit/s. If the line being used is GR2000-1B or an Ethernet with built in GR2000-2B, a maximum transmission band of 80 kbit/s is allocated, even if the band is not set in the queue.

Default: 0

Range of value: 0-100

- When WAN circuits are operating, transmission bandwidth (for PPP, transmission speed, and PVC minimum access rate (min_access_rate) for Frame Relay) and output packet length can cause error rates up to 20 percent. Smaller the bandwidth and longer the output packet length, greater is the possibility of error.

  Default: 0

  Range of value: 0-100

`[-queue_number <Queue Number>]`

Description: Allocates bandwidth to queue 1 through specified queue number equally. Sets only when queue mode is equal_bandwidth. Invalid when queue mode is -priority, -round_robin, -bandwidth, -bandwidth_kbps or -bandwidth_traffic.

Downloaded from www.Manualslib.com manuals search engine

Default: 24

Range of value: 1-32
(Queue cannot to be created to interface depends on the specified value. 1-8 is for queue count 8, 9-16, for 16, and 17-32 for 32. Bandwidth is allocated equally to the specified value within the created queue.)

```
[{-max_queue_number_4 | -max_queue_number_8 | -max_queue_number_16 |
-max_queue_number_32 | -max_queue_number_64 | -max_queue_number_250 |
-max_queue_number_1000}]
```

Description: Specifies the maximum queue count to be created to interface. Invalid when queue mode is -priority, -round_robin, -bandwidth, -equal_bandwidth.

-max_queue_number_4: The maximum queue count is 4.
-max_queue_number_8: The maximum queue count is 8.
-max_queue_number_16: The maximum queue count is 16.
-max_queue_number_32: The maximum queue count is 32.
-max_queue_number_64: The maximum queue count is 64(*1) [ROUTE-OS6B].
-max_queue_number_250: The maximum queue count is 250.
-max_queue_number_1000: The maximum queue count is 1000.
The maximum queue number can be 64 only when set to one line (line number zero).

(*1):The relationship between the "-max" queue number 64 and the set line in GR2000-1B and GR2000-2B is explained below:

1. 64 is effective as the maximum queue number only when set to one line (line number zero.
2. If the "-max" queue number 64 is defined in relation to the line number zero under a condition where multiple line information definitions are set in the same NIF in GR2000-1B and GR2000-2B, this definition is null and void.
3. If the "-max" queue number 64 is defined in the line number zero in GR2000-1B and GR2000-2B, and the "-max" queue number 64 is deleted under a condition where multiple line information definitions are present in the same NIF, use the maintenance free command for other lines.

```
[-queue <Queue No.>, <Queue No.>-<Queue No.>, ... <min rate (kbps)>]
```

Description: Specifies the minimum bandwidth per queue. When only queue No. is specified and the minimum bandwidth is not specified, 0 [kbit/s] is set to minimum bandwidth. The minimum band is set only when the queue mode is bandwidth_kbps. The minimum band is invalid even if it is set when the queue mode is priority, round_robin, bandwidth, or bandwidth_traffic.

To specify the minimum bandwidth of one queue: -queue 5 (Specifies queue No. 5.)

To specify the minimum bandwidth of plural queues: -queue 5, 10, and 12 (Specifies queue No. 5, 10, and 12.)

To specify the minimum bandwidth of a range of queue: -queue 21 to 30 (Specifies queue No. 21 to 30.)

Downloaded from www.Manualslib.com manuals search engine

To specify the minimum bandwidth of plural queues and a range of queues: -queue 1, 3, and 50 to 53 (Specifies queue No. 1, 3, and 50 to 53.)

When queue mode is minimum bandwidth (kbps) and the total bandwidth exceeds the line speed, the bandwidth is allocated sequentially to the guarantee with smaller queue No. within the range of line speed.

Default: 0

Range of value: 0-6144

`-traffic <Queue No.> -constant -peak_rate <kbps>`

This parameter sets the maximum transmission band when securing the fixed band for each queue and transmitting packets. The maximum transmission band is set only when the queue mode is -bandwidth_traffic. The maximum transmission band is invalid even if it is set when the queue mode is -priority, -round_robin, -bandwidth, -equal_bandwidth, or -bandwidth_kbps. Table 1-71 shows the parameters when the queue mode is designated in the band control (traffic designation). Table 1-73: List of the parameters when GR2000-1B and GR2000-2B band designation (traffic designation) is made. This table shows the list of parameters when band control (traffic designation) is designated in GR2000-1B and GR2000-2B.

`-traffic <Queue No.> -garantee -min_rate <kbps> [-peak_rate <kbps>] [-weight <Rate>]`

This parameter sets the assignment ratio of the excess band to be distributed according to the ratio in which the minimum guarantee band, maximum transmission band, and excess band are set for each queue when packets are transmitted for each queue between the minimum guarantee band and maximum transmission band. The assignment ratio is set only when the queue mode is bandwidth_traffic. The assignment ratio is invalid even if it is set when the queue mode is priority, round_robin, bandwidth, equal_bandwidth, or bandwidth_kbps. Table 1-71 shows the parameters when the queue mode is designated in the band control (traffic designation). Table 1-73: List of the parameters when GR2000-1B and GR2000-2B band designation (traffic designation) is made. This table shows the list of parameters when band control (traffic designation) is designated in GR2000-1B and GR2000-2B.

Downloaded from www.Manualslib.com manuals search engine

Table 1-71 Parameters list in bandwidth control (traffic)

Item	Parameter	Support			Description
		10BASE-T	100BASE-TX	1000BASE-SX 1000BASE-LX 1000BASE-LH	
Queue No.	-max_queue_number_8 -max_queue_number_32	8 queue		8, 32 queue	Set the expanded number of queue.
Traffic type per queue	-constant	(1)Fixed band			Set it when the fixed band is ensured.
	-guarantee	(2) Variable band			Set it when the variable band is set.
Minimum guarantee band for each queue (*2) (*3) (*7)	-min_rate	1050kbit/s to 10000kbit/s (*4)	1050kbit/s to 100000kbit/s (*4)	1050kbit/s to 1000000kbit/s (*5)	Set the minimum guarantee band by queues.
Maximum transmission band for each queue (*2) (*3) (*7)	-peak_rate	1050kbit/s to 10000kbit/s (*4)(*6)	1050kbit/s to 100000kbit/s (*4)(*6)	1050kbit/s to 1000000kbit/s (*5)(*6)	Set the maximum transmission band by queues.
Excess band allocation ratio.(*8)	-weight	1 to 63			Distribute and allocate the bands according to the ratio in which the excess band is set by queues.

**1: The router operates in eight queues when the maximum number of queues is not set.*
**2: The maximum transmission band (192 kbit/s) is assigned when no band is set in a queue.*
**3: The maximum error is about 5%.*
**4: The relay performance per NIF is 360 Mbit/s.*
**5: The relay performance of RP-D is 700 Mbit/s. Up to 1 Gbbit/s, no output thus occurs.*
**6: Set the maximum transmission band of a queue as described below when the queue traffic type is specified as guarantee.*
Minimum guarantee band for each queue ≦ Maximum transmission band for each queue ≦ Maximum limitation band of line
**7: The router operates under output priority control when the total number of guaranteed bands specified in each queue exceeds the line rate. The guaranteed band specified in each queue is a maximum transmission band when the traffic type is a fixed band. It is a minimum guarantee band when the traffic type is a variable band. The unspecified queue is 192 kbit/s.*
**8: The excess bandwidth is the bandwidth set from the maximum transmission bandwidth of a line for each queue. For fixed bandwidth, it is the excess bandwidth obtained when the total of the maximum bandwidth is subtracted. For variable bandwidth, it is the excess bandwidth obtained when the total of the minimum guarantee bandwidth is subtracted. The bandwidth is divided and assigned according to the setting value of -weight when excess bandwidth exists. A calculation example of excess bandwidth in a 100BASE-TX line is given below.*

Downloaded from www.Manualslib.com manuals search engine

Table 1-72 Calculation Example of Excess Bandwidth

Traffic Type	Minimum Bandwidth Guarantee (kbit/s)	Maximum Bandwidth Limitation (kbit/s)	Ratio of Excess Bandwidth Assignment	Excess Bandwidth (kps)
-constant	-	192	0	0
-constant	-	10000	0	0
-guarantee	10000	-	1	19424x1/16=1214
-guarantee	20000	-	4	19424x4/16=4856
-constant	-	192	0	0
-guarantee	30000	-	4	19424x4/16=4856
-guarantee	10000	-	7	19424x7/16=8498
Not set.	-	192	0	0

** To set the band control (traffic designation) to a physical line in which a VLAN line is defined, do not change the maximum queue number. If a change is made, close the applicable RP using the GR2000 Operations Commands, Vol. 1,* close rp *command, and then release the closure using the* free rp *command.*

Table 1-73 List of the Parameters When GR2000-1B and GR2000-2B Band Designation (Traffic Designation) is Made.

Item	Parameter	Support			Description
		10BASE-T	100BASE-TX	1000BASE-SX 1000BASE-LX 1000BASE-LH	
Queue No.(*1)	-max_queue_number_4 -max_queue_number_8 -max_queue_number_64(*5)	4, 8, 64 queue			Set the expanded number of queue.
Traffic type per queue	-constant	Fixed band			Set it when the fixed band is ensured.
	-guarantee	Variable band			Set it when the variable band is set.
Minimum guarantee band for each queue (*2) (*4)	-min_rate	80kbit/s - 10000kbit/s	80kbit/s - 10000kbit/s	80kbit/s - 590000kbit/s	Set the minimum guarantee band by queues.
Maximum transmission band for each queue (*2) (*3) (*4)	-peak_rate	80kbit/s - 10000kbit/s	80kbit/s - 10000kbit/s	80kbit/s - 590000kbit/s	Set the maximum transmission band by queues.
Excess band allocation ratio.	-weight	1 to 63			Distribute and allocate the bands according to the ratio in which the excess band is set by queues.

**1: The router operates in four queues when the maximum number of queues is not set.*
**2: The maximum error is about 2%.*
**3: Set the maximum transmission band of a queue as described below when the queue traffic type is specified as guarantee. Minimum guarantee band for each queue ≦Maximum transmission band for each queue ≦Maximum limitation band of line*
**4: The router operates under output priority control when the total number of guaranteed bands specified in each queue exceeds the line rate. The guaranteed band specified in each queue is a maximum transmission band when the traffic type is a fixed band. It is a minimum guarantee band when the traffic type is a variable band. The unspecified queue is 80 kbps.*
**5:The maximum queue number can be 64 only when set to one line (line number zero).*

Downloaded from www.Manualslib.com manuals search engine

Example

1. Setting parameters:

   a. To set the queueA mode for priority:

```
(config)#qos -yes
(config)#qos-queue-list queueA -priority
(config)#show qos-queue-list queueA
       qos_queue_list queueA priority;
(config)#
```

   b. To set the queueB mode for bandwidth (20 percent of bandwidth is allocated to queue1 and 80 percent to queue 2):

```
(config)#qos -yes
(config)#qos-queue-list queueB -bandwidth -queue1_bandwidth 20
\
-queue2_bandwidth 80
(config)#show qos-queue-list queueB
       qos_queue-list queueB bandwidth {
               queue1 bandwidth 20;
               queue2 bandwidth 80;
};
(config)#
```

   c. To set the queueC mode for round-robin:

```
(config)#qos -yes
(config)#qos-queue-list queueC -round_robin
(config)#show qos-queue-list queueC
qos_queue-list queueC round_robin;
(config)#
```

   d. To set the queueD mode for equal minimum bandwidth and allocate bandwidth equally by 28 queue:

```
(config)#qos -yes
(config)#qos-queue-list queueD -equal_bandwidth -queue_number 28
(config)#show qos-queue-list queueD
       qos_queue-list queueD equal_bandwidth queue_number 28;
(config)#
```

   e. To set minimum bandwidth of queue No. 1 to 800 to 5 kbit/s and 801 to 1000 to 10 kbit/s when interface count is 1000:

```
(config)#qos-queue-list QUE1 -bandwidth_kbps -max_queue_number_1000
(config)#qos-queue-list QUE1 -queue 1-800 5
(config)#qos-queue-list QUE1 -queue 801-1000 10
(config)#show qos-queue-list QUE1
       qos_queue-list QUE1 bandwidth_kbps {
            max_queue_number_1000;
            queue 1-800 5;
            queue 801-1000 10;
       };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

f. Set the queue mode of queue list name QUEUEF to the band control (traffic designation). Assign a fixed band of 1 Mbit/s to queue number 1. Assign a minimum guarantee band of 1.5 Mbit/s and a maximum limitation band of 9 Mbit/s to queue number 2. Assign a minimum guarantee band of 6 Mbit/s and a maximum limitation band of 9 Mbit/s to queue number 3.

```
(config)# qos -yes
(config)# qos-queue-list QUEUEF -bandwidth_traffic 100000
(config)# qos-queue-list QUEUEF -ttraffic 1 -constant -peak_rate 1000
(config)# qos-queue-list QUEUEF -ttraffic 2 -guarantee -min_rate 1500
-peak_rate 9000
(config)# qos-queue-list QUEUEF -ttraffic 3 -guarantee -min_rate 6000
-peak_rate 9000
(config)# show qos-queue-list QUEUEF
        qos_queue_list QUEUEF bandwidth_traffic 100000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee peak_rate 9000 min_rate 1500;
                traffic 3 guarantee peak_rate 9000 min_rate 6000;
        };
```

g. Set the queue mode of queue list name QUEUEG to the band control (traffic designation) and set the number of queues to 32. Assign a fixed band of 10 Mbit/s to queue numbers 1 through 8. Assign a fixed band of 20 Mbit/s to queue numbers 9 and 10.

```
(config)# qos -yes
(config)# qos-queue-list QUEUEG -bandwidth_traffic 100000
-max_queue_number 32
(config)# qos-queue-list QUEUEG -ttraffic 1 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 2 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 3 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 4 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 5 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 6 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 7 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 8 -constant -peak_rate 10000
(config)# qos-queue-list QUEUEG -ttraffic 9 -constant -peak_rate 20000
(config)# qos-queue-list QUEUEG -ttraffic 10 -constant -peak_rate 20000
(config)# show qos-queue-list QUEUEG
        qos_queue_list QUEUEG bandwidth_traffic 100000 {
                max_queue_number_32;
                traffic 1 constant peak_rate 10000;
                traffic 2 constant peak_rate 10000;
                traffic 3 constant peak_rate 10000;
                traffic 4 constant peak_rate 10000;
                traffic 5 constant peak_rate 10000;
                traffic 6 constant peak_rate 10000;
                traffic 7 constant peak_rate 10000;
                traffic 8 constant peak_rate 10000;
                traffic 9 constant peak_rate 20000;
                traffic 10 constant peak_rate 20000;
        };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Modifying parameters:

   To modify queueB bandwidth for queue1 and queue2 to 10 percent and 90 percent, respectively:

```
(config)#show qos-queue-list queueB
       qos_queue-list queueB bandwidth {
               queue1 bandwidth 20;
               queue2 bandwidth 80;
       };
(config)#qos-queue-list queueB -bandwidth -queue1_bandwidth
10 -queue2_bandwidth 90
(config)#show qos-queue-list queueB
       qos_queue-list queueB bandwidth {
               queue1 bandwidth 10;
               queue2 bandwidth 90;
       };
(config)#
```

   a. Change the maximum limitation band of queue number 2 in queue list name QUEUEF, whose queue mode is set to the band control (traffic designation), from 9 Mbit/s to 5 Mbit/s.

```
(config)# show qos-queue-list QUEUEF
        qos_queue_list QUEUEF bandwidth_traffic 100000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee peak_rate 9000 min_rate 1500;
                traffic 3 guarantee peak_rate 9000 min_rate 6000;
        };
(config)# qos-queue-list QUEUEF -traffic 2 -peak_rate 5000
(config)# show qos-queue-list QUEUEF
        qos_queue_list QUEUEF bandwidth_traffic 100000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee peak_rate 5000 min_rate 1500;
                traffic 3 guarantee peak_rate 9000 min_rate 6000;
        };
(config)#
```

3. Displaying settings:

   a. To display all settings:

```
(config)#show qos-queue-list
       qos_queue_list queueA priority ;
       qos_queue_list queueB bandwidth {
               queue1 bandwidth 10;
               queue2 bandwidth 20;
       };
       qos_queue_list queueC round_robin;
(config)#
```

   b. To display any queue list name:

```
(config)#show qos-queue-list queueA
       qos_queue_list queueA priority;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Deleting settings:

   a. To delete queue list name queue A:

```
(config)#show qos-queue-list
       qos_queue_list queueA priority;
       qos_queue_list queueC round_robin;
(config)#delete qos-queue-list queueA
(config)# show qos-queue-list
       qos_queue_list queueC round_robin;
(config)#
```

5. Deleting parameter:

   a. To delete queue1_bandwidth of queueB. Qos-queue-list parameter that once set can be deleted by delete command.

```
(config)#show qos-queue-list queueB
       qos_queue_list queueB bandwidth {
           queue1_bandwidth 20;
           queue2_bandwidth 80;
       };
(config)#delete qos_queue_list queueB -queue1_bandwidth
(config)#show qos-queue-list queueB
       qos_queue_list queueB bandwidth {
              queue2_bandwidth 80;
       };
(config)#
```

   b. To delete queue2_bandwidth of queueB. Qos-queue-list parameter that once set can be deleted by specifying parameter name.

```
(config)# show qos-queue-list QUEUEF
        qos_queue_list QUEUEF bandwidth_traffic 100000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee peak_rate 5000 min_rate 1500;
                traffic 3 guarantee peak_rate 9000 min_rate 6000;
        };
(config)# delete qos-queue-list QUEUEF -traffic 2 -peak_rate
(config)# show qos-queue-list QUEUEF
        qos_queue_list QUEUEF bandwidth_traffic 100000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee min_rate 1500;
                traffic 3 guarantee peak_rate 9000 min_rate 6000;
        };
(config)#
```

   c. Deletes queue number 3 of queue list name QUEUE in which the queue mode is set to band control (traffic designation).

```
(config)# show qos-queue-list QUEUEF
         qos_queue_list QUEUEF bandwidth_traffic 100000 {
                 traffic 1 constant peak_rate 1000;
                 traffic 2 guarantee min_rate 1500;
                 traffic 3 guarantee min_rate 6000 peak_rate 9000;
         };
(config)# delete qos-queue-list QUEUEF traffic 3
(config)# show qos-queue-list QUEUEF
        qos_queue_list QUEUEF bandwidth_traffic 100000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee min_rate 1500;
        };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

qos
qos-interface
qos-discard-mode
qos-ip-list
qos-ip-list-group
qos-tos-map
qos-ip
qos-ipx
qos-bridge
qos-hdlc

Precautions

1. When changing a queue mode, perform new setting after deleting the related parameters.
2. The active attribute list on the QoS interface cannot be deleted.
3. When allocates QoS queue attribute with -bandwidth_kbps queue mode to interface by qos-interface command, the maximum number of usable queue is 4000 per RP. Set the total queue count dedicated to each interface to be 4000 or less per RP according to the below. The queue count dedicated to one interface becomes the following by the setting of max_queue_number_N of allocated QoS queue attribute information.
   -max_queue_number_8 ---------- 250
   -max_queue_number_16 ---------- 250
   -max_queue_number_32 ---------- 250
   -max_queue_number_250 ---------- 250
   -max_queue_number_1000 ---------- 1000
   For example, the interface using QoS queue attribute of minimum bandwidth (kbit/s) that specified -max_queue_number_8, -max_queue_number_16, -max_queue_number_32, or -max_queue_number_250 can be set up to 16 lines per RP. The interface using QoS queue attribute of minimum bandwidth (kbit/s) that specified -max_queue_number 1000 can be set up to 4 lines per RP. When total queue count to be dedicated by QoS queue attribute of minimum bandwidth (kbit/s) exceeds 4000 per RP, minimum bandwidth guarantee (kbit/s) cannot be processed in the part of interface within the target RP.
4. The storage conditions on the performance and loading memory are provided when using a QoS queue attribute list. Refer to the *GR2000 Installation Guide*.
5. With the interface having set the queue mode to -bandwidth_kbps (minimum band assurance (specified by kbit/s)) and -bandwidth_traddic (band control (specified traffic)) by using this command, the minimum band assurance (kbit/s specified) and -bandwidth_traddic (band control (specified traffic)) function can be executed only when the output priority is decided by output priority specification using the flow control. If the output priority has been decided by DSCP value by using the flow control, the minimum band assurance (kbit/s specified) and -bandwidth_traddic (band control (specified traffic)) function cannot be executed. Table 1-74 shows the relationship between the minimum band assurance (kbit/s specified) and -bandwidth_traddic (band control (specified traffic)), and the flow control.
6. This command cannot be set when a -cops parameter is set to qos (QoS information).
7. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP

Downloaded from www.Manualslib.com manuals search engine

routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

8. When the queue mode is set to the band control (traffic designation) using this command, set in the same line so that the total of min_rate for the queue of which traffic type is guarantee, peak_rate for the queue of which traffic type is constant, and 192 kbit/s for the queue of which traffic type is not set becomes less than the maximum transmission band of a line.
9. If addition/deletion/change in the parameters is executed in the qos-queue-list (QoS attribute) in NE100-STB, communication in all of the lines in the same NIF is temporarily disabled.

Table 1-74 Relationship Between Priority Determination Among Minimum Bandwidth Guarantee (kbit/s), Band Control (Traffic Designation), and Flow Control

Method for Deciding Priority in Flow Control	Subject Configuration Command	Subject Parameter	Advisability of Executing Functions of the Minimum Bandwidth Guarantee (kbit/s designation), and Band Control (Traffic Designation)
Designation for out put priority	qos-ip-list	priority_class	√
	flow qos	priority	√
Designation for DSCP rewritten value	filter-list	replace_tos	x
	qos-ip-list	replace_tos	x
	flow filter	replace_dscp	x
	flow qos	replace_tos	x
Designation for input packet DSCP value	qos-ip-list	tos-map	x
	flow qos	tos-map	x

√: Execution possible x : Execution impossible.
*(*1): Only PR-A1 can be executed.*

1.2.3 qos-interface

Applies the QoS queue list to an interface. A maximum of 480 entries may be created for each RP.

Input Format

Setting information

```
[set] qos-interface {<Line Name> | <DLCI Name> | <Timeslot Name> | <Peer
Name> | <VLAN Name>} -queue_list <Queue-List-Name>
[set] qos-interface <Line Name> -group <No.> -peak_rate <kbps>
[-traffic <Queue No.> -constant -peak_rate <kbps>]
[-traffic <Queue No.> -guarantee  -min_rate <kbps>
[-peak_rate <kbps>] [-weight <Rate>]]
[set] qos-interface <VLAN Name> -peak_rate <kbps>
[-traffic <Queue No.> -constant -peak_rate <kbps>]
[-traffic <Queue No.> -guarantee  -min_rate <kbps>
[-peak_rate <kbps>] [-weight <Rate>]]
```

Modifying information

```
[set] qos-interface {<Line Name> | <DLCI Name> | <Timeslot Name> | <Peer
Name> | <VLAN Name>} -queue_list <Queue-List-Name>
```


Downloaded from www.Manualslib.com manuals search engine

```
[set] qos-interface <Line Name> -group <No.> [-peak_rate <kbps>]
[-traffic <Queue No.> [-constant] -peak_rate <kbps>]
[-traffic <Queue No.> [-guarantee] [-min_rate <kbps>]
[-peak_rate <kbps>] [-weight <Rate>]]
[set] qos-interface <VLAN Name> [-peak_rate <kbps>]
[-traffic <Queue No.> [-constant] -peak_rate <kbps>]
[-traffic <Queue No.> [-guarantee] [-min_rate <kbps>]
[-peak_rate <kbps>] [-weight <Rate>]]
```

Deleting information

```
delete qos-interface {<Line Name> | <DLCI Name> | <Timeslot Name> | <Peer Name> | <VLAN Name>}
delete qos-interface <Line Name> [-group <No.> [-traffic <Queue No.>]]
delete qos-interface <VLAN Name> [-traffic <Queue No.>]
```

Displaying information

```
show qos-interface [{ <Line Name> | <DLCI Name> | <Timeslot Name> | <Peer Name> | <VLAN Name>}]
show qos-interface <Line Name> [-group <No.>]
```

Table 1-75 shows the parameters that can be set by each transmission control.

Table 1-75 Parameters That Can be Set by Each Transmission Control

Parameter	Sending Control						
	Output Priority Control	Minimum Bandwidth Guarantee	Round-robin	Uniform minimum band guarantee	Minimum Bandwidth Guarantee (specified in kbit/s)	Bandwidth control (specified in traffic)	Group bandwidth control
<Line Name>	√	√	√	√	√(*1)	√(*2)	√(*4)
<DLCI Name>	√	√	√	√	--	--	--
<Timeslot Name>	√	√	√	--	√(*1)	--	--
<Peer Name>	√	√	√	--	--	--	--
<VLAN Name>	√	--	--	--	--	√(*3)	√(*4)
-queue_list <Queue-List-Name>	√	√	√	√	√	√	--
-queue_list <Queue-List-Name>	--	--	--	--	--	--	√(*4)
-group <No.>	--	--	--	--	--	--	√(*4)
-peak_rate <kbps>	--	--	--	--	--	--	√(*4)
-traffic <Queue No.> -constant-peak_rate <kbps>	--	--	--	--	--	--	√(*4)

√: Usable
-: Unusable
**1: Only a slow-speed WAN line can be set.*
**2: Only an Ethernet line and a Gigabit Ethernet line can be set.*
**3: Only VLAN lines in GR2000-1B and GR2000-2B can be set.*
**4: Only Ethernet lines and Gigabit Ethernet lines in GR2000-1B and GR2000-2B can be set.*

Downloaded from www.Manualslib.com manuals search engine

Parameters

```
{ <Line Name> | <DLCI Name> | <Timeslot Name> | <Peer Name> }
```

This parameter specifies the interface name for the interface that sets QoS queue attributes. The following table displays various interface names along with the circuits and protocols that the interfaces supports.

Table 1-76 Interface Names

Interface	Circuits (Protocols)
<Line Name>	OC-3c, OC-12c, OC-48c, serial (PPP), T3, E3, Ethernet, Gigabit Ethernet
<DLCI Name>	DLCI (Frame Relay [*1])
<Timeslot Name>	BRI (PPP), PRI (PPP), J2 (PPP), T1 (PPP), E1 (PPP)
<Peer Name>	ISDN
<VLAN Name>	VLAN [ROUTE-OS6B]
**1: Frame Relay circuits can be specified only by <DLCI Name>.*	

Default: None; only the displayed value is supported.

```
-queue_list <Queue-List-Name>
```

This parameter specifies the queue list name. (QoS queue attributes must be set before this command is invoked.)

Default: None

Range of value: Character strings must begin with an alphabetic character and contain no more than 14 characters.

```
-group<No.> [ROUTE-OS6B]
```

Group numbers are set.

Default: No default is allowed.

Range of value: The value setting range varies depending on the number of physical lines that set the group band control in the same NIF. Table 1-77 shows the relationship between the physical line that sets the group band control in the same NIF and the group number that can be set.

Table 1-77 Relationship Between the Physical Line That Sets the Group Band Control in the Same NIF and the Group Number That Can Be Set

Physical line that sets the group band control.	Number of Groups	
	Physical line that sets the group band control in the same NIF	
	One line	All lines
Line number zero	1 - 16 (*1)	1 - 2
Line number other than zero	-- (*1)	1 - 2
**1: If a group number greater than three is set, communication is possible only through line number zero.*		

Downloaded from www.Manualslib.com manuals search engine

`-peak_rate <kbps> [ROUTE-OS6B]`

The maximum transmission band is set to the VLAN line or the group.

Default: None

Range of value: The value setting range varies by each line type.

Table 1-78 shows the range in which a line's maximum transmission range can be set.

Table 1-78 Range in Which a Line's Maximum Transmission Range Can Be Set

No.	NIF Type	Line Type	Available Range
1	GR2000-1B	10BASE-T full-duplex	320 - 10000
2	GR2000-2B	100BASE-TX full-duplex	320 - 100000
3	Ethernet containing NEB100-4TB NEB1G-1B (*)	1000BASE-SX 1000BASE-LX 1000BASE-LH	320 - 590000
*: NEB1G-1B can be set at up to 590 Mbit/s.			

`-traffic <Queue No.> -constant -peak_rate <kbps> [ROUTE-OS6B]`

The maximum transmission band is set when the fixed band assures each queue will transmit a packet. Table 1-79 shows the list of the parameters.

Table 1-79 List of Parameters When the Band Control (Traffic Designation) in the VLAN Line or the Group Band Control is Designated

Item	Parameter	Support			Description
		10BASE-T	100BASE-TX	1000BASE-SX 1000BASE-LX 1000BASE-LH	
Queue No.(*1)	-traffic	1 to 4(*1)			Sets the queue number.
Traffic type per queue	-constant	Fixed band			Set it when the fixed band is ensured.
	-guarantee	Variable band			Set it when the variable band is set.
Minimum guarantee band for each queue (*2) (*4)	-min_rate	80 kbit/s - 10000 kbit/s	80 kbit/s - 10000 kbit/s	80 kbit/s - 590000 kbit/s	Set the minimum guarantee band by queues.
Maximum transmission band for each queue (*2) (*3) (*4)	-peak_rate	80 kbit/s - 10000 kbit/s	80 kbit/s - 10000 kbit/s	80 kbit/s - 590000 kbit/s	Set the maximum transmission band by queues.
Excess band allocation ratio.	-weight	1 to 63			Distribute and allocate the bands according to the ratio in which the excess band is set by queues.

**1: The VAN line or the group set at four queues.*
**2: The maximum error is about 2%.*
**3: Set the maximum transmission band of a queue as described below when the queue traffic type is specified as guarantee. Minimum guarantee band for each queue ≦ Maximum transmission band for each queue ≦ Maximum limitation band of line*
**4: The router operates under output priority control when the total number of guaranteed bands specified in each queue exceeds the line rate. The guaranteed band specified in each queue is a maximum transmission band when the traffic type is a fixed band. It is a minimum guarantee band when the traffic type is a variable band. The unspecified queue is 80 kbps.*

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Setting parameters:

   a. When the interface name is <Line Name>: Ethernet circuit, NIF number 0, LINE number 0, LINE name: priority on office 1 specifies the QoS queue list name queueA:

```
(config)# line office1 ethernet 0/0
(config)# qos -yes
(config)# qos-queue-list queueA -priority
(config)# qos-interface office1 -queue_list queueA
(config)# show qos-interface
       qos_interface office1 queue_list queueA ;
(config)#
```

   b. When the interface name is <DLCI Name>: serial circuit, NIF number 1, LINE number 0, line speed 9600bps, LINE name: office2, protocol: Frame Relay, DLCI number 16, DLCI name: round-robin on dlci1 specifies the QoS queue list name queue B:

```
(config)# line office2 serial 1/0 line_speed 9.6
(config)# frame-relay office2
(config)# dlci office2 dlci1 16
(config)# qos -yes
(config)# qos-queue-list queueB -round_robin
(config)# qos-interface dlci1 -queue_list queueB
(config)# show qos-interface
       qos_interface dlci1 queue_list queueB;
(config)#
```

   c. When the interface name is <Timeslot Name>: J2 circuit, NIF number 2, LINE number 0, LINE name: office3, timeslot number 1, timeslot width 1, timeslot name: section1, protocol : priority on PPP specifies QoS queue list name queueC:

```
(config)# line office3 j2 2/0
(config)# timeslot office3 section1 1 width 1
(config)# ppp section1
(config)# qos -yes
(config)# qos-queue-list queueC -priority
(config)# qos-interface section1 -queue_list queueC
(config)# show qos-interface
       qos_interface section1 queue_list queueC;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

d. The QoS queue list name "QUEUED" is set using the band control (traffic designation) in the Ethernet line, NIF number zero, LINE number zero if the interface name is <VLAN Name>, the LINE name: center, VLAN ID: 10 and VLAN name: "office1."

```
(config)# line center ethernet 0/0 -type 10m_fullduplex
(config)# vlan center office1 10
(config)# qos -yes
(config)# qos-queue-list QUEUED -bandwidhth_traffic 10000
(config)# qos-queue-list QUEUED -traffic 1 -constant -peak_rate 1000
(config)# qos-queue-list QUEUED -traffic 2 -constant -peak_rate 2000
(config)# qos-queue-list QUEUED -traffic 3 -constant -peak_rate 3000
(config)# qos-queue-list QUEUED -traffic 4 -constant -peak_rate 4000
(config)# qos-interface office1 -queue_list QUEUED
(config)# show -r line center
line center ethernet 0/0 {
        vlan office1 10 {
        };
};
qos yes {
        qos_queue_list QUEUED bandwidth_traffic 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 constant peak_rate 2000;
                traffic 3 constant peak_rate 3000;
                traffic 4 constant peak_rate 4000;
        };
        qos_interface office1 queue_list QUEUED;
};
(config)#
```

e. Set the parameter using the band control (traffic designation) in the Ethernet line, NIF number zero, LINE number zero if the interface name is <VLAN Name>, the LINE name: center, VLAN ID: 10 and VLAN name: "office1.

```
(config)# line center ethernet 0/0 -type 100m_fullduplex
(config)# vlan center office1 10
(config)# qos -yes
(config)# qos-interface office1 -peak_rate 10000
(config)# qos-interface office1 -traffic 1 -constant -peak_rate 1000
(config)# qos-interface office1 -traffic 2 -constant -peak_rate 2000
(config)# qos-interface office1 -traffic 3 -constant -peak_rate 3000
(config)# qos-interface office1 -traffic 4 -constant -peak_rate 4000
(config)# show -r line center
line center ethernet 0/0 type 100m_fullduplex {
        vlan office1 10 {
        };
};
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 constant peak_rate 2000;
                traffic 3 constant peak_rate 3000;
                traffic 4 constant peak_rate 4000;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

f. Set the parameter using the band control (traffic designation) in the Ethernet line, NIF number zero, LINE number zero if the interface name is <VLAN Name>, the LINE name: office1.

```
(config)# line office1 ethernet 0/0 -type 100m_fullduplex
(config)# qos -yes
(config)# qos-interface office1 -group 1 -peak_rate 10000
(config)# qos-interface office1 -group 1 -traffic 1 -constant -peak_rate 10
(config)# qos-interface office1 -group 1 -traffic 2 -constant -peak_rate 20
(config)# qos-interface office1 -group 1 -traffic 3 -constant -peak_rate 30
(config)# qos-interface office1 -group 1 -traffic 4 -constant -peak_rate 40
(config)# qos-interface office1 -group 2 -peak_rate 20000
(config)# qos-interface office1 -group 2 -traffic 1 -guarantee -min_rate 80
(config)# qos-interface office1 -group 2 -traffic 2 -guarantee -min_rate 60
(config)# qos-interface office1 -group 2 -traffic 3 -guarantee -min_rate 40
(config)# qos-interface office1 -group 2 -traffic 4 -guarantee -min_rate 20
(config)# show -r line office1
line center office1 0/0 type 100m_fullduplex;
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 2 constant peak_rate 2000;
                        traffic 3 constant peak_rate 3000;
                        traffic 4 constant peak_rate 4000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Modifying parameters:

   a. To modify the QoS queue list name on interface name office1 from queueA to queue B:

```
(config)# show qos-interface office1
        qos_interface office1 queue_list QUEUEA ;
(config)# qos-interface office1 -queue_list QUEUEB
(config)# show qos-interface office1
        qos_interface office1 queue_list QUEUEB ;
(config)#
```

   b. The maximum limitation band of queue number 2 in the interface name: "office1" that has set the band control (traffic designation) is changed from 2Mbit/s to 4Mbit/s.

```
(config)# show qos-interface office1
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 constant peak_rate 2000;
                traffic 3 constant peak_rate 2000;
                traffic 4 constant peak_rate 3000;
        };
};
(config)# qos-interface office1 -traffic 2 -peak_rate 4000
(config)# show qos-interface office1
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 constant peak_rate 4000;
                traffic 3 constant peak_rate 2000;
                traffic 4 constant peak_rate 3000;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

c. The maximum limitation band of queue number 2 in the interface name: "office1" and " group1" that has set the group band control is changed from 2Mbit/s to 4Mbit/s.

```
(config)# show qos-interface office1
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 2 constant peak_rate 2000;
                        traffic 3 constant peak_rate 2000;
                        traffic 4 constant peak_rate 3000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
(config)# qos-interface office1 -group 1 -traffic 2 -peak_rate 4000
(config)# show qos-interface office1
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 2 constant peak_rate 4000;
                        traffic 3 constant peak_rate 2000;
                        traffic 4 constant peak_rate 3000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
(config)#
```

3. Displaying settings:

a. To display all settings:

```
(config)# show qos-interface
       qos_interface office1 queue_list QUEUEB;
       qos_interface dlci1 queue_list QUEUEB;
       qos_interface section1 queue_list QUEUEC;
(config)#
```

b. To display any interface setting:

```
(config)# show qos-interface office1
        qos_interface office1 queue_list QUEUEB;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Deleting settings:

   a. To delete the QoS queue list setting for interface name office1:

```
(config)# show qos-interface
        qos_interface office1 queue_list QUEUEB;
        qos_interface office2 queue_list QUEUEB;
(config)# delete qos-interface office1
(config)# show qos-interface
        qos_interface office2 queue_list QUEUEB;
(config)#
```

   b. The maximum limitation band of queue number 2 in the interface name: "office1" that has set the band control (traffic designation) is deleted.

```
(config)# show qos-interface office1
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee min_rate 4000 peak_rate 8000;
                traffic 3 constant peak_rate 2000;
                traffic 4 constant peak_rate 3000;
        };
};
(config)# delete qos-interface office1 -traffic 2 -peak_rate
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee min_rate 4000;
                traffic 3 constant peak_rate 2000;
                traffic 4 constant peak_rate 3000;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

c. The maximum limitation band of queue number "two" in the interface names: "office1" and "group 1" that have set the group band control is deleted.

```
(config)# show qos-interface office1
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 2 guarantee min_rate 4000 peak_rate 8000;
                        traffic 3 constant peak_rate 2000;
                        traffic 4 constant peak_rate 3000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
(config)# delete qos-interface office1 -group 1 -traffic 2 -peak_rate
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 2 guarantee min_rate 4000;
                        traffic 3 constant peak_rate 2000;
                        traffic 4 constant peak_rate 3000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
(config)#
```

d. The queue number 2 in the interface name: "office1" that has set the band control (traffic designation) is deleted.

```
(config)# show qos-interface office1
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 2 guarantee min_rate 4000 peak_rate 8000;
                traffic 3 constant peak_rate 2000;
                traffic 4 constant peak_rate 3000;
        };
};
(config)# delete qos-interface office1 -traffic 2
qos yes {
        qos-interface office1 peak_rate 10000 {
                traffic 1 constant peak_rate 1000;
                traffic 3 constant peak_rate 2000;
                traffic 4 constant peak_rate 3000;
        };
};
```


Downloaded from www.Manualslib.com manuals search engine

e. To delete the queue number "two" in the interface names: "office1" and "group 1" that have set the group band control.

```
(config)# show qos-interface office1
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 2 guarantee min_rate 4000 peak_rate 8000;
                        traffic 3 constant peak_rate 2000;
                        traffic 4 constant peak_rate 3000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
(config)# delete qos-interface office1 -group 1 -traffic 2
qos yes {
        qos-interface office1 {
                group 1 peak_rate 10000 {
                        traffic 1 constant peak_rate 1000;
                        traffic 3 constant peak_rate 2000;
                        traffic 4 constant peak_rate 3000;
        };
                group 2 peak_rate 20000 {
                        traffic 1 guarantee min_rate 8000;
                        traffic 2 guarantee min_rate 6000;
                        traffic 3 guarantee min_rate 4000;
                        traffic 4 guarantee min_rate 2000;
        };
};
```

Related Commands

qos
qos-queue-list
qos-discard-mode
qos-ip-list
qos-ip-list-group
qos-tos-map
qos-ip
qos-ipx
qos-bridge
qos-hdlc, line, timeslot, ppp, frame-relay, dlci

Precautions

1. This command cannot be used with ATM.
2. When the operating configurations stored in memory are modified, the modified interfaces will restart. Use caution when logged in through a network.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
4. This command cannot be set when a -cops parameter is set to qos (QoS information).

Downloaded from www.Manualslib.com manuals search engine

5. If addition/deletion/change in the parameters is executed in the qos-interface (QoS interface information) in the Ethernet (NE100-8TB), communication in all of the lines in the same NIF is temporarily disabled.
6. With the interface that has used this command to set the group band control, the group band control function can be executed only when the output priority has been determined using the output priority designation in the flow control. If the DSCP rewriting has been designated in the flow control or if the output priority has been determined by the input packet DSCP value designation, the group band control function cannot be executed. Table 1-80 shows the relationship between the group band control and the flow control in priority determination.

Table 1-80 Relationship in the priority determination between the group band control and the flow control

Method for Deciding Priority in Flow Control	Subject Configuration Definition Information	Subject Parameter	Advisability of Executing Functions of the Group Band Control
Designation for out put priority	qos-ip-list	priority_class	x
	flow qos	priority	√
Designation for DSCP rewritten value	filter-list	replace_tos	x
	qos-ip-list	replace_tos	x
	flow filter	replace_tos	x
	flow qos	replace_tos	x
Designation for input packet DSCP value	qos-ip-list	tos-map	x
	flow qos	tos-map	x

√: Execution possible x : Execution impossible.

7. When setting the group band control, the following restrictions shall apply:

- It is necessary to set the control to a physical line in which no VLAN line has been set.
- When setting the group number three and higher, set the control only to the line with line number zero. If the group number three or higher has been set, only the line number zero will be able to communicate.

8. When setting the band control (traffic designation) in the VLAN line, the following restrictions shall apply:

- It is necessary that no transmission control other than the complete priority control be set to a physical line on the VLAN line.
- When setting a VLAN line greater than three lines to an interface in which the band control (traffic designation) in the VLAN line has been set, choose only the line with the line number zero. If a VLAN line greater than three lines has been set, only the line with the line number zero is able to communicate.

9. It may not be possible to guarantee the specified bandwidth if bandwidth control (traffic specified) or group bandwidth control is specified in Gigabit Ethernet and the flow control function is enabled.

Downloaded from www.Manualslib.com manuals search engine

1.2.4 qos-discard-mode

This command sets the discard mode to a NIF, where discard mode is queue size. The discard mode enables queuing by priority class.

Input Format

Setting information

```
[set] qos-discard-mode -nif < NIF No. > -discard_mode < Discard Mode >
```

Modifying information

```
[set] qos-discard-mode  -nif < NIF No. > -discard_mode < Discard Mode >
```

Deleting information

```
delete qos-discard -nif < NIF No. >
```

Displaying information

```
show qos-discard
```

Parameters

`-nif <NIF No.>`

Description: Specifies the NIF number

Default: None; only the displayed value is supported

range of value: For the range of NIF numbers that can be specified, see *GR2000 Configuration Commands, (universal CLI) Vol. 1*.

`-discard_mode <Discard Mode>`

Description: Specifies the discard mode.

Table 1-81 Discard Mode

Discard	**Priority Class**			
Mode	**1**	**2**	**3**	**4**
0	**1-8**	2-8	3-8	8-8
1	1-8	3-8	5-8	8-8
2	2-8	4-8	6-8	8-8
3	3-8	5-8	7-8	8-8
Note: The n-8 entries indicate how full the queue is; i.e., queue size.				

Default: 3

Range of value: 0-3

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Setting parameters:

   To set discard mode 2 on NIF number 9:

```
(config)# qos -yes
(config)# qos-discard-mode -nif 9 -discard_mode 2
(config)# show qos-discard-mode
       qos_discard_mode nif 9 discard_mode 2;
(config)#
```

2. Modifying parameters:

   To change discard mode on NIF number 9 from 2 to 1:

```
(config)# show qos-discard-mode
       qos_discard_mode nif 9 discard_mode 2;
(config)# qos-discard-mode -nif 9 -discard-mode 1
(config)#  show qos-discard-mode
       qos_discard_mode nif 9 discard_mode 1;
(config)#
```

3. Displaying settings:

   To display settings:

```
(config)# show qos-discard-mode
       qos_discard_mode nif 1 discard_mode 1;
       qos_discard_mode nif 9 discard_mode 2;
(config)#
```

4. Deleting settings:

   To delete the NIF discard mode setting:

```
(config)# show qos-discard-mode
       qos_discard_mode nif 1 discard_mode 1;
       qos_discard_mode nif 9 discard_mode 1;
(config)# delete qos-discard-mode -nif 1
(config)# show qos-discard-mode
       qos_discard_mode nif 9 discard_mode 1;
(config)#
```

Related Commands

qos
qos-queue-list
qos-interface
qos-ip-list
qos-ip-list-group
qos-tos-map
qos-ip

Precautions

1. This command cannot be used with ATM.
2. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

1.2.5 *qos-ip-list* (Information on QoS IP Frame Condition of the Old BSD UNIX-Based Command System)

This sets IP QoS information. QoS ip frame condition groups are assigned to interfaces defined by ip information or ip-address information. If IP QoS information is set, QoS determination is executed in sent or received packets of the relevant interface. It is possible to set a maximum of 512 entries per device (maximum 256 interfaces with inbound and outbound for each interface).

Input Format

Setting/modifying information

```
[set] qos-ip-list <IP List No.> [-protocol <No.>]
[{-payload_length_upper_limit | -payload_length_lower_limit} <Payload
Length>]
[-tos <Value>]
[{-ip_pair | -ip_pair_off}]
[-ip_source <IP Address> [{-<IP Address> | mask <Subnet Mask> | masklen
<Subnet Mask Bit Length> | /<Subnet Mask Bit Length>}]] [-ip_destination
<IP Address> [{-<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask
Bit Length> | /<Subnet Mask Bit Length>}]]
[{-port_pair | -port_pair_off}]
[-port_source <Port No.> [-<Port No.>]] [-port_destination <Port No.>
[-<Port No.>]]
[{-pair_synchronized_off | -pair_synchronized}]
[-icmp_type <No.>] [-icmp_code <No.>] [-igmp_type <No.>] [-branch_index
<No.>]
[-exp <value>]
[{-max_rate_importance | -max_rate_normal | -min_rate_importance |
-min_rate_normal}]
[-upc_group_no <No.>]
[{-max_priority_class_8 | -max_priority_class_16 |
-max_priority_class_32}]
[{[[-priority_class <No.>] [-discard_class <No.>] [-upc {no |
<Bandwidth>}
[-upc_penalty {drop | -modified_priority_class <No.>
-modified_discard_class <No.>}]]]
| [[-replace_tos <New_Tos Value>] [-upc {no | <Bandwidth>}
[-upc_penalty {drop | <Modified_New_Tos Value>}]]]
| [[-tos_map] [-upc {no | <Bandwidth>}
[-upc_penalty {drop | <Modified_New_Tos Value>}]]]
| [[-replace_exp <Value>] [-priority_class <NO.>] [-discard_class <NO.>]]
}]
[-burst_size <Byte>]
```

Deleting information

```
delete qos-ip-list < IP List No. >
```

Displaying information

```
show qos-ip-list [< IP List No. >]
```

Displaying all free entry No.

```
show qos-ip-list free
```


Downloaded from www.Manualslib.com manuals search engine

Displaying the first free entry No.

```
show qos-ip-list free min_no
```

TCP, UDP, and other upper level protocols specify the configurable parameters for flow detection, whereas the flow control parameters that can be configured depend on the type of flow-control process used. The following tables illustrate the configurable parameters for flow detection that are supported by various upper-level protocols, and the flow-control parameters that are supported by different flow-control methods. IP QoS settings are generated by selecting one parameter type from the flow-detection parameter table (see Table 1-82) and one from the flow-control type parameter table (see Table 1-83 to create one entry.

Table 1-82 Configurable Parameters for Flow Detection by Upper-level Protocol

Flow-Detection Parameter	Upper-Level Protocol					
	TCP	UDP	ICMP	IGMP	Unspecified	Other
<IP List No.>	††	††	††	††	††	††
-protocol <No.>	6	17	1	2		†
{-payload_length_upper_limit | -payload_length_lower_limit} <Payload Length>	†	†	†	†	†	†
-tos <Value>	†	†	†	†	†	†
{-ip_pair | -ip_pair_off}	*	*	*	*	*	*
-ip_source <IP Address> -<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Lendth>]	†	†	†	†	†	†
-ip_destination <IP Address> -<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Lendth>]	†	†	†	†	†	†
{-port_pair | -port_pair_off}	*	*				
-port_source <Port No.> [-<Port No.>]	†	†				
-port_destination <Port No.> [-<Port No.>]	†	†				
{-pair_synchronized_off | -pair_synchronized}	*	*				
-icmp_type <No.>			†			
-icmp_code <No.>			†			
-igmp_type <No.>				†		
*††: required, †: configurable, *: configurable; default, blank: not configurable, numeral: numeric setting*						

Downloaded from www.Manualslib.com manuals search engine

Table 1-83 Configurable Flow Control Parameters by Flow-control Type

Flow Control Parameter	Condition 1			Condition 2			Condition 3			Condition 4	Condition 5
	1-1	1-2	1-3	2-1	2-2	2-3	3-1	3-2	3-3	4-1	5-1
-max_priority_class_X	*	*	*								
-priority_class <No.> -discard_class <No.>	*	*	*							*	*
-replace_tos <New_Tos Value>				††	††	††					
-tos_map							††	††	††		
-upc {no | <Bandwidth>}	*(1)	††(2)	††(2)	*(1)	††(2)	††(2)	*(1)	††(2)	††(2)		
-upc_penalty drop		*			*			*			
-upc_penalty -modified_priority_class <No.> -modified_discard_class <No.>			††								
-upc_penalty <Modified_New_Tos Value>						††			††		
-replace_exp <Value>										††	

*††: required, †: configurable, *: configurable; default, blank: not configurable, numeral: numeric setting*
1: no (or default value)
2: requires a numeric value

Flow control may be classified into three types by transmission priority:

- Condition 1: Precedence not determined by TOS.
- Condition 2: TOS is rewritten; converted TOS determines precedence.
- Condition 3: Precedence determined by input IP packet TOS.
- Condition 4: Determines the EXP and priority level.
- Condition 5: Determines the priority level by EXP.

Flow control is further classified using the following three conditions:

- Condition 1: No reserve bandwidth management.
- Condition 2: Detected flows that violate bandwidth reservation are discarded.
- Condition 3: When a detected flow violates bandwidth reservation, its priority is lowered.

Parameters

`<IP List No.>`

Description: This parameter specifies the QoS IP frame condition list number.

Default: Only in display. The entire QoS IP frame condition list is displayed.

Range of value: `1-1024`

Flow Detection Condition Parameters

`-protocol <No.>`

Description: This parameter specifies an upper-level protocol.

Downloaded from www.Manualslib.com manuals search engine

Default: None (upper-level protocols are not flow-detection conditions).

Range of value: 0-255

```
{ -payload_length_upper_limit | -payload_length_lower_limit } <Payload
Length>}
```

Description: This parameter specifies IP user data length upper and lower limits.

`payload_length_upper_limit`
Specifies IP user data length upper limit.

`payload_length_lower_limit`
Specifies IP user data length lower limit.

Table 1-84 Relationship Between IP User Data Length Upper/Lower Limits and IP User Total Data Length

Upper/Lower Limit Specification	Relation between packet value A (packet value= total length - header length) and configured IP user data length B	Result
-payload_length_upper_limit	A < or = B	Match
-payload_length_upper_limit	A > B	Mismatch
-payload_length_lower_limit	A > or = B	Match
-payload_length_lower_limit	A < B	Mismatch

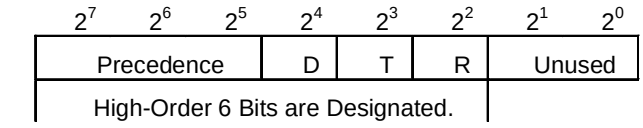
Default: None (IP user data length upper and lower limit values are not flow detection conditions).

Range of value: 0-65535

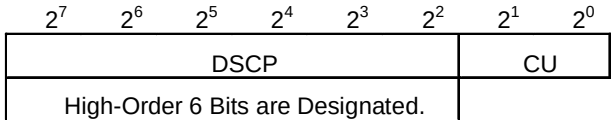
```
-tos <Value>
```

Description: This parameter specifies values corresponding to the 6 high-order bits in a TOS field or a DS field of Diff-serv, and compares these to the 6 high-order bits of a received packet TOS field or a DS field of Diff-serv.

The two low-order bits are ignored; specification is invalid.



D (Delay), T (Throughput), R (Reliability)



DSCP (Differentiated Services Code Point), CU (Current Unused)

Default: None (TOS values are not flow detection conditions).

Range of value: 0-255 (see note 2)

Downloaded from www.Manualslib.com manuals search engine

{ -ip_pair | -ip_pair_off }

Description: This parameter specifies a method to check IP source and destination addresses.

-ip_pair
Switches IP source and destination addresses for an address check, then runs a check without switching the addresses (see note 1).

-ip_pair_off
Checks IP source and destination addresses without switching the addresses.

Before specifying the -ip_pair check, set the synchronized check function for IP address and upper level protocol port number to OFF (-pair_synchronized_off).

Default: -ip_pair

-ip_source <IP Address> [-<IP Address> | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]]

Description: This parameter specifies the IP source address. A single address is specified as -ip_source <IP Address>. An address range is specified as -ip_source <lower limit IP Address> - <upper limit IP Address>, -ip_source mask <Subnet Mask>, -ip_source masklen <Subnet Mask Bit Length>, or -ip_source/<Subnet Mask Bit Length>.

Default: None (IP source address is not a flow detection condition).

Range of value: 0.0.0.0-255.255.255.255

-ip_destination <IP Address> [-<IP Address>] | mask <Subnet Mask> | masklen <Subnet Mask Bit Length> | /<Subnet Mask Bit Length>]]

Description: This parameter specifies the IP destination address. When both source and destination IP addresses are set under one condition, set so that the specified addresses do not overlap. If they overlap, set an IP address pair switch as ip-pair-off.
A single address is specified as -ip_destination <IP Address>. An address range is specified as -ip_destination <lower limit IP Address> - <upper limit IP Address>, -ip_destination mask <Subnet Mask>, -ip_destination masklen <Subnet Mask Bit Length, or -ip_destination/ <Subnet Mask Bit Length>.

Default: None (IP destination address is not a flow detection condition).

Range of value: 0.0.0.0-255.255.255.255

{ -port_pair | -port_pair_off }

Description: This parameter specifies a method to check upper-level protocol port numbers of source and destination protocols.

-port_pair
Checks upper-level protocol port numbers without the port numbers of the source and destination protocols, then switches port numbers and runs the protocol port number check again (see note 1).

Downloaded from www.Manualslib.com manuals search engine

-port_pair_off
Checks upper-level protocol port numbers without switching the port numbers of the source and destination protocols.

Before specifying the -port_pair check, set the synchronized check function for IP address and upper level protocol port number to OFF (-pair_synchronized_off).

Define 6 (TCP) or 17 (UDP) for a -protocol parameter when this parameter is specified. The set value of this parameter is disabled when a -protocol parameter is undefined or when 6 (TCP) or 17 (UDP) is not defined.

Default: -port_pair

-port_source <Port No.> [-<Port No.>]

Description: This parameter specifies the port number of an upper-level source protocol. One port number is specified as -port_source <Port No.>. A port number range is specified as -port_source <lower limit Port No.> - <upper limit Port No.>. When both source and destination upper protocol port numbers are set under one condition, set so that the specified upper protocol port numbers do not overlap. If they overlap, set an upper protocol port number's pair switch as port_pair_off.

Define 6 (TCP) or 17 (UDP) for a -protocol parameter when this parameter is specified. The set value of this parameter is disabled when a -protocol parameter is undefined or when 6 (TCP) or 17 (UDP) is not defined.

Default: None (source port numbers are not flow detection conditions).

Range of value: 0-65535

-port_destination <Port No.> [-<Port No.>]

Description: This parameter specifies the port number of an upper-level destination protocol. One port number is specified as -port_source <Port No.>. A range is specified as -port_source <lower limit Port No.> - <upper limit Port No.>. When both destination and source upper protocol port numbers are set under one condition, set so that the specified upper protocol port numbers do not overlap. If they overlap, set an upper protocol port number's pair switch as port_pair_off.

Default: None.

Range of value: 0-65535

{ -pair_synchronized_off | -pair_synchronized }

Description: This parameter specifies a synchronized check of IP addresses and upper-level protocol port numbers.

-pair_synchronized_off
Checks the source and the destination IP addresses, and upper-level source and destination protocol port numbers without simultaneously switching the values. Note that the IP and/or port check will follow the routine of -ip_ pair and/or -port_pair if either or both of those parameters are specified.

Downloaded from www.Manualslib.com manuals search engine

-pair_synchronized
Checks the source and the destination IP addresses, and upper-level source and destination protocol port numbers by simultaneously switching the values (synchronized check). To run the synchronized source and destination IP address check, specify: -ip_pair_off. For the synchronized port number check, specify: -port_pair_ off (see note 1).

Default: -pair_synchronized_off

-icmp_type <No.>

Description: This parameter specifies the ICMP type.

Default: None (ICMP type is not a flow detection condition).

Range of value: 0-255

-icmp_code <No.>

Description: This parameter specifies the ICMP code.

Default: None (ICMP code is not a flow detection condition).

Range of value: 0-255

-igmp_type <No.>

Description: This parameter specifies the IGMP type.

Default: None (IGMP type is not a flow detection condition).

Range of value: 0-255

Table 1-85 List of IGMP Type Number

IGMP Type No. (HEX)	Input Value (Decimal)	Name
0x11	17	Membership Query
0x12	18	Version 1 Membership Report
0x13	19	DVMRP protocol
0x16	22	Version 2 Membership Report
0x17	23	Version 2 Leave Group
0x22	34	Version 3 Membership Report

-branch_index <No.>

Description: This parameter specifies a connection branch Index number (DLCI group information or Index specified using VC-Group information). This parameter selects and sends the specified DLCI/VC information in a group when it relays a packet that coincides with QoS IP frame conditions. For the QoS IP frame conditions under which the connection branch Index number is set, specify parameter -out (Outbound) and set it as QoS IP frame conditions on the output side when setting IP QoS information. See 1.2.8 in this guide.

Default: None

Range of value: 0-7

Downloaded from www.Manualslib.com manuals search engine

-exp <Value>

Description: This parameter specifies an EXP field value. The number of packets that coincide with the flow detection conditions is not displayed.

Default: None (EXP is not contained in flow detection conditions.)

Range of value: 0-7

Flow Control Parameters

Flow control parameter

[{-max_rate_importance | -max_rate_normal | -min_rate_importance | -min_rate_normal}]

This parameter sets whether the contents of the band control set in this list are a minimum guarantee band or maximum limitation band and whether the flow is an important packet or normal packet when important packet protection (priority band assignment) is performed in each band.

-max_rate_importance:

When the flow detected in this list is an important packet in a maximum limitation band

-max_rate_normal:

When the flow detected in this list is a normal packet in a maximum limitation band

-min_rate_importance:

When the flow detected in this list is an important packet in a minimum guarantee band

-min_rate_normal:

When the flow detected in this list is a normal packet in a minimum guarantee band

Default

None (The band control and important packet protection described above are not performed.)

This parameter conforms to the conditions below when it is used.

- Put the flow control parameter (UPC) of an important packet and normal packet into the same setting state when performing important packet protection.
- The upc_penalty operation when this parameter is set is as shown in the table below.

Downloaded from www.Manualslib.com manuals search engine

Table 1-86 UPC Penalty Operation

	Default Operation	Change Method
Maximum band limitation (Important)	Drop	Cannot be changed.
Maximum band limitation (Normal)	Drop	Cannot be changed.
Minimum band guarantee (Important)	-modified_discard_class 1 *1	Specified by -modified_discard_class <No.>.
Minimum band limitation (Normal)	-modified_discard_class 1 *1	Specified by -modified_discard_class <No.>. *2
*1: -modified_priority_class uses the class specified by -priority_class. *2: Uses -modified_discard_class <No.> set in a minimum band guarantee (important) list.		

- Change it with the list to be changed not registered in qos-ip-list-group when changing this parameter.
- The flow control parameter below uses the setting value specified in an important packet when a normal packet is specified in this parameter.

  `-tops_map,-priority_class,-discard_class,-replace_tos,-upc_penalty`
- This parameter is valid only in RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B and GR2000-2B.

`[upc_group_no <No.>]`

Description: This parameter sets the same group number in units of groups that control a band.

Default: None (A band is not controlled in units of groups.)

Range of value: 1-2000 (decimal)

A list with the same number operates as an identical band control group when the list in which this parameter is specified is set to qos-ip-list-group.

This parameter conforms to the conditions below when it is used.

- Change it with the list to be changed not registered in qos-ip-list-group when changing this parameter.
- The maximum number of lists that can be handled as one group is four.
- Set and delete a list to and from qos-ip-list-group continuously for each group number in the order below.
- This parameter is valid only in RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B and GR2000-2B.

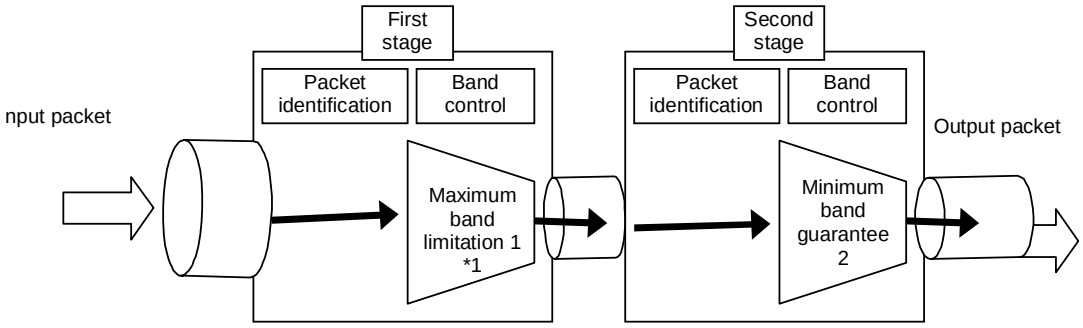
Downloaded from www.Manualslib.com manuals search engine

Table 1-87 UPC Combined Setting Sequence

Combined Setting	Setting Sequence			
	(1)	(2)	(3)	(4)
Maximum band limitation	- max_rate_importance	-	-	-
Minimum band guarantee	- min_rate_importance	-	-	-
Maximum band limitation + Minimum guarantee band	- max_rate_importance	- max_rate_importance	-	-
Maximum band limitation + Important packet protection	- max_rate_importance	- max_rate_normal	-	-
Minimum guarantee band + Important packet protection	- min_rate_importance	min_rate_normal	-	
Maximum band limitation + Minimum guarantee band + Important packet protection	- min_rate_importance	max_rate_normal	- min_rate_importance	min_rate_normal

The setting contents of this parameter, and the setting sequence and control points of a list are shown below (1 to 4).

- Maximum band limitation + Minimum band guarantee (Maximum band limitation only or minimum band guarantee only)



*1: For only the maximum band limitation or minimum band guarantee, only 1 is set.

Figure 1-9 Maximum Band Limitation + Minimum Band Guarantee

Downloaded from www.Manualslib.com manuals search engine

- Maximum band limitation + Important packet protection or Minimum band guarantee + Important packet protection

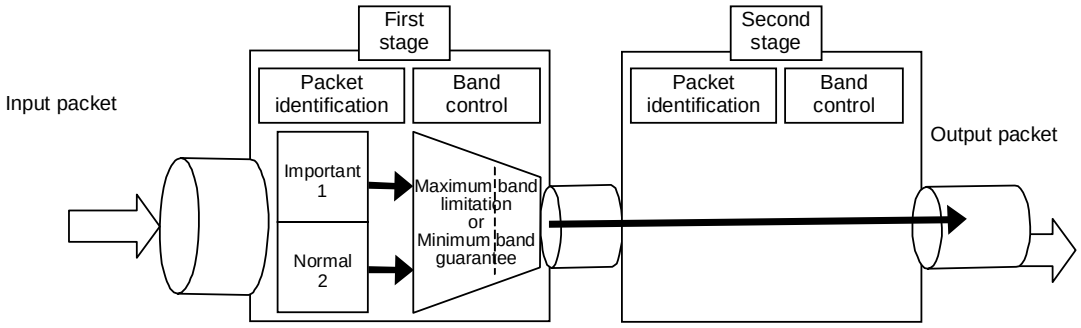


Figure 1-10 Maximum Band Limitation + Important Packet Protection

- Maximum band limitation + Minimum band guarantee + Important packet protection

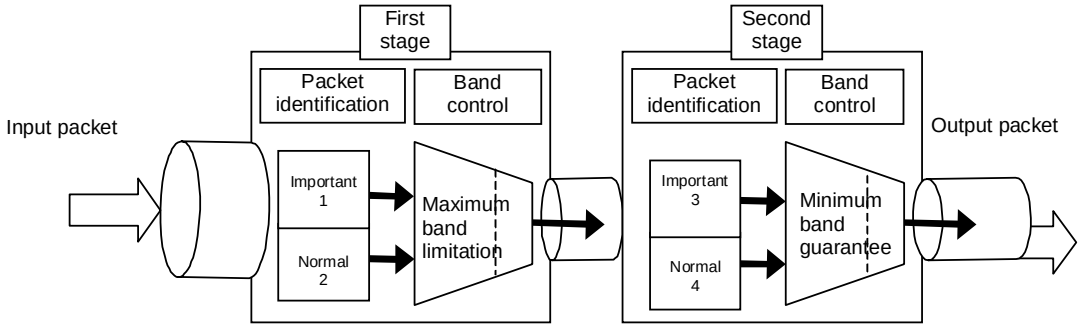


Figure 1-11 Maximum Band Limitation + Minimum Band Guarantee + Important Packet Protection

`[{-max_priority_class_8 | -max_priority_class_16 | -max_priority_class_32}]`

Description: Specifies maximum output priority.
-max_priority_class_8: The maximum output priority is 8.
-max_priority_class_16: The maximum output priority is 16.
-max_priority_class_32: The maximum output priority is 32.

Default: When using this list in input side: 8
When using this list in output side: The number of queue of output interface
(When this parameter is omitted, maximum class of output priority is dynamically changed at the change of queue count of output interface. Omitting of this parameter is recommended.)

`[-priority_class <No.>] [-discard_class <No.>]`

Description: This parameter enables flow control through output priority class and discard class queuing mechanisms. The value set for `<No.>` in this parameter represents priority.

For purposes of output precedence, the `-priority_class` parameter indicates output priority. However, when used in respect to minimum bandwidth guarantee (the bandwidth queue mode), it functions as the queue number.

Note that when this parameter is active, the parameters `-replace_tos` and `-tos_map` cannot be specified.

Downloaded from www.Manualslib.com manuals search engine

Default: `-priority_class 4 -discard_class 4`

range of value: `-priority_class <No.>:1-8`

(In terms of priority, higher the priority value of a packet, the greater is the output priority.)

`-discard_class <No.>:1-4`

(In terms of discard, lower the priority value of a packet, greater is the discard priority.)

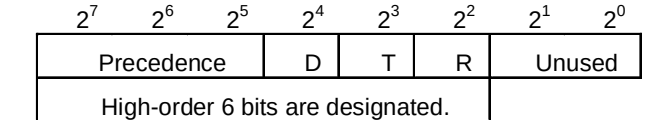
Table 1-88 Range of Priority Class and Discard Class

Setting Condition			Range	
Max. Output Priority	**Interface Using This List**	**Queue Count of Output Interface**	**Output Priority**	**Queuing Priority**
Omitted	Input side	—	1-8	1-4
Omitted	Output side	8	1-8	1-4
Omitted	Output side	16	1-16	1-4
Omitted	Output side	32	1-32	1-4
Omitted	Output side	250	1-250	1-4 (*2)
Omitted	Output side	1000	1-1000	1-4 (*2)
8	--	--	1-8	1-4
16	--	--	1-16	1-4
32	--	--	1-32	1-4

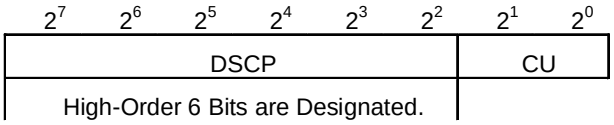
**1: When the value other than the range is specified to output priority, the setting becomes invalid.*
**2: When QoS queue attribute of output interface is minimum bandwidth guarantee (kbit/s), flow control is processed as follows:*
- *Queuing priority 1, 2: Flow control is processed by queuing priority 2.*
- *Queuing priority 3, 4: Flow control is processed by queuing priority 4.*

`-replace_tos <New_Tos Value>`

Description: This parameter makes valid the flow control function replaced by TOS or DS field of Diff-serv. Sets the number of bits replacing TOS or DS field of Diff-serv. The upper 6 bits of the TOS or DS field of Diff-serv field are replaced. The lower 2 bits are ignored even if this parameter is set. When this parameter is set, `-priority_class`, `-discard_class`, and `-tos_map` cannot be set.



D (Delay), T (Throughput), R (Reliability)



DSCP (Differentiated Services Code Point), CU (Current Unused)

Downloaded from www.Manualslib.com manuals search engine

Default: -priority_class 4 -discard_class 4(output priority class, flow control set by queuing priority class)

range of value: -replace_tos <New_Tos Value>:0-255 (Note 2)

[-tos_map]

Description: This parameter makes the function of QoS control by TOS input valid.

When this parameter is set, -priority_class, -discard_class, and -replace_tos cannot be set.

Default: -priority_class 4 -discard_class 4
(output priority class, flow control by setting queuing priority class)

-upc {no | <Bandwidth>}

Description: This parameter sets the use of the agreed band monitoring function and the agreed band.

no: Unused

<Bandwidth>: Sets the agreed band in bit/s. If the number is greater than the circuit speed, performance ends.

Default: -upc no

Range of value: <Bandwidth>:0-1000000000(0-1G)

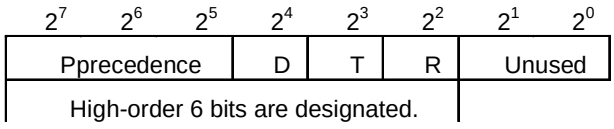
If a number from 0-11999 is set, performance continues, as the contract field is 12000 [bit/s].

-upc_penalty {drop | <Modified_New_Tos Value> | -modified_discard_class<No.> -modified_priority_class <No.>}

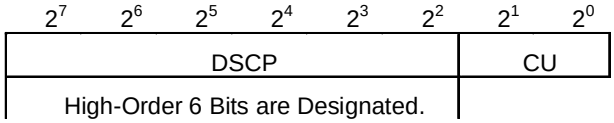
Description: This parameter sets the performance at the time of the violation of the agreed band.

drop: Drops the frame.

<Modified_New_Tos Value>:
Sets the number replacing TOS or DS field of Diff-serv, and QoS control by replaced TOS or DS field of Diff-serv. The upper 6 bits of the TOS or DS field of Diff-serv field are replaced. The lower 2 bits are ignored even if this parameter is set.



D (Delay),T (Throughput), R (Reliability)



DSCP (Differentiated Services Code Point), CU (Current Unused)

Downloaded from www.Manualslib.com manuals search engine

-modified_priority_class <No.>:

Sets the output priority class after changes. Used as the output priority class when the output priority control is used, and used as a queue number when the bandwidth and round-robin scheme are used.

-modified_discard_class<No.>:

Sets the queuing priority after changes.

Default: -upc_penalty drop

Range of value: <value>0-255

-modified_priority_class <No.>1-8

-modified_discard_class <No.>1-4

Table 1-89 Range of Priority Class and Discard Class

Setting Condition			Range	
Max. Output Priority	**Interface Using This List**	**Queue Count of Output Interface**	**Output Priority**	**Queuing Priority**
Omitted	Input side	--	1-8	1-4
Omitted	Output side	8	1-8	1-4
Omitted	Output side	16	1-16	1-4
Omitted	Output side	32	1-32	1-4
Omitted	Output side	250	1-250	1-4 (*2)
Omitted	Output side	1000	1-1000	1-4 (*2)
8	--	--	1-8	1-4
16	--	--	1-16	1-4
32	--	--	1-32	1-4

**1: When the value other than the range is specified to output priority, the setting becomes invalid.*
**2: When queue count of output interface is 250 or 1000, flow control is processed as follows:*
- *Queuing priority 1, 2: Flow control is processed by queuing priority 2.*
- *Queuing priority 3, 4: Flow control is processed by queuing priority 4.*

-replace_exp <Value>

Description: This parameter specifies the rewrite value of an EXP field.

Default: None

Range of value: 0-7

-burst_size <Byte>

Description: his parameter sets the burst size in units of bytes during band monitoring.

Default: None (The burst size is not considered during band monitoring.)

Range of value: 1 to 131,072 (decimal)

- This parameter is validated in lists other than the normal packet of maximum band limitation or minimum band guarantee.
- This parameter is valid only in RP-C, RP-D, RP-C6, RP-D6, RP-CV, RP-DV, GR2000-1B and GR2000-2B.

Downloaded from www.Manualslib.com manuals search engine

Notes

1. When using IP address pair switch, higher protocol port No, pair switch, or IP address higher protocol No. interlock switch, pay attention to the followings:

- When address pair switch is used with “-ip_pair”.

  To use source IP address and destination IP address by specifying the range, set not to overlap the ranges of source IP address and destination IP address.

- When address pair switch is used with “-port_pair”.

  To use source higher protocol No. and destination higher protocol No. by specifying the range, set not to overlap the ranges of source higher protocol No. and destination higher protocol No.

- When using by combining pair switches.

  When combining IP address pair switch, higher protocol port No, pair switch, and IP address higher protocol No. interlock switch, use them in the combination shown in Tables 1-90 and 1-91. The setting values of an upper protocol port number’s pair switch and IP address upper protocol number’s interlock pair switch are validated when 6(TCP) or 17(UDP) is defined in the upper protocol number. The setting values of an upper protocol port number’s pair switch and IP address upper protocol number’s interlock pair switch are invalidated when the upper protocol number is undefined or when numbers other than 6(TCP) or 17(UDP) are defined in the upper protocol number.

Table 1-90 Combination of Pair Switch

No.	Combination of Pair Switch			Setting	Processing
1	-Pair_synchronized_off	-port_pair_off	-ip_pair_off	Available	Checks the O‘ address and high-order protocol port No. by not switching source and destination.
2			-ip_pair	Available	The source and destination upper protocol port numbers are checked without being replaced. Checks the source IP address by both cases of switching/not switching source and destination.
3		-port_pair	-ip_pair_off	Available	Checks the source high-order protocol No. by both cases of switching/not switching source and destination. The source and destination IP addresses are checked without being replaced.
4			-ip_pair	Available (Default)	For the IP address and upper protocol port number, the source and destination are checked in both cases below. • When they are not replaced • When they are replaced
5	-pair_synchronized	-port_pair_off	-ip_pair_off	Available	For the IP address and upper protocol port number, the source and destination are checked in the cases below. • When both of them are not replaced • When both of them are replaced at the same time.
6			-ip_pair	Not available	—
7		-port_pair	-ip_pair_off	Not available	—
8			-ip_pair	Not available	—

Downloaded from www.Manualslib.com manuals search engine

When the upper protocol number is undefined or when numbers other than 6(TCP) or 17(UDP) are defined in the upper protocol number.

Table 1-91 Combined Setting of Pair Switch and Possibility of Use

Item	Combined Setting of Pair Switch (Note 2)	Possibility of Use	Processing
1	-ip_pair_off	Possible	The source and destination IP addresses are checked without being replaced. • Possible
2	-ip_pair	Possible	The source and destination IP addresses are checked in both cases below. • When they are not replaced • When they are replaced
**: -port_pair_off / -port_pair and -pair_synchronized_off/-pair_synchronized switches are invalidated when the upper protocol number is undefined or when numbers other than 6(TCP) or 17(UDP) are defined in the upper protocol number.* *The calculation expression for obtaining a TOS value is as follows:* *TOS value = precedence (0-7) x 32 (Delay (0, 1) x 16 (Throughput (0, 1) x 8 (Reliability (0, 1) x 4* *A calculation example of the TOS value is shown below.*			

2. The formula to calculate the TOS number is:

```
TOS number=precedence(0-7)x32+Delay(0,1)x16+
Throughput(0,1)x8+Reliability(0,1)x4
```

Examples of the calculated TOS number are shown below.

Table 1-92 TOS Number Calculation

Precedence	Delay	Throughput	Reliability	TOS Number
0	0	0	0	0
1	0	0	0	32
2	0	0	0	64
3	0	0	0	96
4	0	0	0	128
5	0	0	0	160
6	0	0	0	192
7	0	0	0	224

3. The upper 6 bits of the TOS field are replaced and the lower 2 bits are ignored even if this parameter is set. Table 1-93 shows the TOS replacing value for setting value. TOS value of output packet is the one that added TOS value lower 2 bits of output value to TOS replacing value. Replacing of DS field of Diff-serv is executed by the same condition for TOS replacement.

Downloaded from www.Manualslib.com manuals search engine

Table 1-93 TOS Replacing Value for Setting Value

Setting Value	TOS Replacing Value	Setting Value	TOS Replacing Value	Setting Value	TOS Replacing Value
0-3	0	88-91	88	176-179	176
4-7	4	92-95	92	180-183	180
8-11	8	96-99	96	184-187	184
12-15	12	100-103	100	188-191	188
16-19	16	104-107	104	192-195	192
20-23	20	108-111	108	196-199	196
24-27	24	112-115	112	200-203	200
28-31	28	116-119	116	204-207	204
32-35	32	120-123	120	208-211	208
36-39	36	124-127	124	212-215	212
40-43	40	128-131	128	216-219	216
44-47	44	132-135	132	220-223	220
48-51	48	136-139	136	224-227	224
52-55	52	140-143	140	228-231	228
56-59	56	144-147	144	232-235	232
60-63	60	148-151	148	236-239	236
64-67	64	152-155	152	240-243	240
68-71	68	156-159	156	244-247	244
72-75	72	160-163	160	248-251	248
76-79	76	164-167	164	252-255	252
80-83	80	168-171	168		
84-87	84	172-175	172		

4. When specifying the maximum output priority and output interface queue count be sure that the class count and queue count match. If not, class No. and queue No. are mapped and distribute packets to each queue. Mapping class and queue numbers is listed in Table 1-94,

   a. When the maximum output priority is 8:

Table 1-94 Mapping of Class No. and Queue No. (Max Output Priority is 8)

Class No.	Queue No.		
	Queue Count: 8 (matched)	Queue Count: 16 (unmatched)	Queue Count: 32 (unmatched)
1	1	1	1
2	2	3	5
3	3	5	9
4	4	7	13
5	5	9	17
6	6	11	21
7	7	13	25
8	8	15	29

Downloaded from www.Manualslib.com manuals search engine

b. When the maximum output priority is 16:

Table 1-95 Mapping of Class No. and Queue No. (Max Output Priority is 8)

Class No.	Queue No.		
	Queue Count: 8 (matched)	Queue Count: 16 (unmatched)	Queue Count: 32 (unmatched)
1	1	1	1
2	1	2	3
3	2	3	5
4	2	4	7
5	3	5	9
6	3	6	11
7	4	7	13
8	4	8	15
9	5	9	17
10	5	10	19
11	6	11	21
12	6	12	23
13	7	13	25
14	7	14	27
15	8	15	29
16	8	16	31

Downloaded from www.Manualslib.com manuals search engine

c. When the maximum output priority is 32:

Table 1-96 Mapping of Class No. and Queue No. (Max Output Priority is 32)

Class No.	Queue No.		
	Queue Count: 8 (matched)	Queue Count: 16 (unmatched)	Queue Count: 32 (unmatched)
1	1	1	1
2	1	1	2
3	1	2	3
4	1	2	4
5	2	3	5
6	2	3	6
7	2	4	7
8	2	4	8
9	3	5	9
10	3	5	10
11	3	6	11
12	3	6	12
13	4	7	13
14	4	7	14
15	4	8	15
16	4	8	16
17	5	9	17
18	5	9	18
19	5	10	19
20	5	10	20
21	6	11	21
22	6	11	22
23	6	12	23
24	6	12	24
25	7	13	25
26	7	13	26
27	7	14	27
28	7	14	28
29	8	15	29
30	8	15	30
31	8	16	31
32	8	16	32

1. Sets only when output line protocol is frame relay.

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Set parameter:

   Sets the parameter of the flow detection condition and flow control parameter in QoS IP frame condition list number 1.5

   - Flow detection condition parameter
   - The higher priority protocol 6 (TCP),
   - TOS field 32 (precedence:1 Delay:0 Throughput:0 Reliability:0),
   - ip_pair,
   - Source IP address 123.123.1.1-123.123.1.123,
   - Destination IP address 123.123.2.1,
   - port_ pair,
   - The higher priority source protocol board number20-21 (ftp_data, ftp),

   The flow control parameter:

   - TOS replacing number 240 (precedence:7 Delay:1 Throughput:0 Reliability:0),
   - The agreed band100000bit/s,
   - In case of an agreed band violation drop (frame is dropped)
   - config:qos -yes
   - config:qos-ip-list 1 -protocol 6 -tos 32 -ip_pair -ip_source 123.123.1.1 \
   - 123.123.1.123 -ip_destination 123.123.2.1 -port_pair -port_source 20 -21 \
   - replace_tos 240 -upc 1000000 -upc_penalty drop

```
(config)# qos -yes
(config)# qos-ip-list 1 -protocol 6 -tos 32 -ip_pair -ip_source
123.123.1.1 \
-123.123.1.123 -ip_destination 123.123.2.1 -port_pair -port_source 20
-21 \
-replace_tos 240 -upc 1000000 -upc_penalty drop
(config)# show qos-ip-list 1
       qos_ip_list 1 {
              protocol 6;
              tos 32;
              ip_pair;
              ip_source 123.123.1.1-123.123.1.123;
              ip_destination 123.123.2.1;
              port_pair;
              port_source 20-21;
              replace_tos 240 upc 1000000 upc_penalty drop;
     };
(config)#
```

```
config> qos -yes
config> qos-ip-list 1 -ip_destination 123.123.1.1 -upc 5000000
-max_rate_importance -upc_group_no 1
config> qos-ip-list 2 -ip_destination 123.123.1.1 -upc 100000
-min_rate_importance -upc_group_no 1
```


Downloaded from www.Manualslib.com manuals search engine

a. Maximum band limitation + Minimum band guarantee
A flow detection condition parameter and flow control parameter are set in QoS IP frame condition list numbers 1 and 2 for maximum band limitation and minimum band guarantee.

Flow detection condition parameter

Destination IP address: 123.123.1.1

Flow control parameter

Contract band: 5,000,000 bit/s (Maximum limitation band)

Contract band: 100,000 bit/s (Minimum guarantee band)

```
config> qos -yes
config> qos-ip-list 1 -ip_destination 123.123.1.1 -upc 5000000
-max_rate_importance -upc_group_no 1
config> qos-ip-list 2 -ip_destination 123.123.1.1 -upc 100000
-min_rate_importance -upc_group_no 1
config> qos-ip-list-group RedGroup 1
config> qos-ip-list-group RedGroup 2
config> qos-ip Tokyo -out -ip_list_group RedGroup
config> show qos
qos yes {
        qos_ip_list 1 {
                tos 224;
                ip_destination 123.123.1.1;
                upc 5000000;
                max_rate_importance;
                upc_group_no 1;
        };
        qos_ip_list 2 {
                tos 0;
                ip_destination 123.123.1.1;
                upc 5000000;
                max_rate_normal;
                upc_group_no 1;
        };
        qos_ip_list_group RedGroup {
                ip_list 1;
                ip_list 2;
        };
        qos_ip Tokyo out ip_list_group RedGroup;
};
config>
```

b. Maximum limitation band + Important packet protection
A flow detection condition parameter and flow control parameter are set in QoS IP frame condition list numbers 1 and 2 for maximum band limitation and important packets protection.

Flow detection condition parameter of important packet

Destination IP address: 123.123.1.1

TOS field: 224

Flow detection condition parameter of normal packet

Destination IP address: 123.123.1.1

TOS field: 0

Downloaded from www.Manualslib.com manuals search engine

Flow control parameter:

Contract band: 5,000,000 bit/s (Maximum limitation band)

```
config> qos -yes
config> qos-ip-list 1 -ip_destination 123.123.1.1 -tos 224 -upc 5000000
-max_rate_importance -upc_group_no 1
config> qos-ip-list 2 -ip_destination 123.123.1.1 -tos 0 -upc 5000000
-max_rate_normal -upc_group_no 1
config> qos-ip-list-group RedGroup 1
config> qos-ip-list-group RedGroup 2
config> qos-ip Tokyo -out -ip_list_group RedGroup
config> show qos
qos yes {
        qos_ip_list 1 {
                tos 224;
                ip_destination 123.123.1.1;
                upc 5000000;
                max_rate_importance;
                upc_group_no 1;
        };
        qos_ip_list 2 {
                tos 0;
                ip_destination 123.123.1.1;
                upc 5000000;
                max_rate_normal;
                upc_group_no 1;
        };
        qos_ip_list_group RedGroup {
                ip_list 1;
                ip_list 2;
        };
        qos_ip Tokyo out ip_list_group RedGroup;
};
config>
```

c. A flow detection condition parameter and flow control parameter are set in QoS IP frame condition list numbers 1 to 4 for maximum band limitation, minimum band guarantee and each important packets protection.

Flow detection condition parameter of priority packet

Destination IP address: 10.10.10.1

TOS: 224

Flow detection condition parameter of non-priority packet

Destination IP address: 10.10.10.1

TOS: 0

Flow control parameter

Contract band: 5,000,000 bit/s (Maximum limitation band)

Contract band: 100,000 bit/s (Minimum guarantee band)

Downloaded from www.Manualslib.com manuals search engine

```
config> qos -yes
config> qos-ip-list 1 -ip_destination 10.10.10.1 -tos 224 -upc 5000000
-max_rate_importance -upc_group_no 1
config> qos-ip-list 2 -ip_destination 10.10.10.1 -tos 0 -upc 5000000
-max_rate_normal -upc_group_no 1
config> qos-ip-list 3 -ip_destination 10.10.10.1 -tos 224 -upc 100000
-min_rate_importance -upc_group_no 1
config> qos-ip-list 4 -ip_destination 10.10.10.1 -tos 0 -upc 100000
-min_rate_normal -upc_group_no 1
config> qos-ip-list-group RedGroup 1
config> qos-ip-list-group RedGroup 2
config> qos-ip-list-group RedGroup 3
config> qos-ip-list-group RedGroup 4
config> qos-ip Tokyo -out -ip_list_group RedGroup
config> show qos
qos yes {
        qos_ip_list 1 {
                ip_destination 10.10.10.1;
                tos 224;
                upc 5000000;
                max_rate_importance;
                upc_group_no 1;
        };
        qos_ip_list 2 {
                ip_destination 10.10.10.1;
                tos 0;
                upc 5000000;
                max_rate_normal;
                upc_group_no 1;
        };
        qos_ip_list 3 {
                ip_destination 10.10.10.1;
                tos 224;
                upc 100000;
                min_rate_importance;
                upc_group_no 1;
        };
        qos_ip_list 4 {
                ip_destination 10.10.10.1;
                tos 0;
                upc 100000;
                min_rate_normal;
                upc_group_no 1;
        };
        qos_ip_list_group RedGroup {
                ip_list 1;
                ip_list 2;
                ip_list 3;
                ip_list 4;
        };
        qos_ip Tokyo out ip_list_group RedGroup;
};
config>
```


Downloaded from www.Manualslib.com manuals search engine

2. Modify parameters:

```
(config)# show qos-ip-list 1
  qos_ip_list 1 {
       protocol 6;
     tos 32;
       ip_pair;
     ip_source 123.123.1.1-123.123.1.123;
       ip_destination 123.123.2.1;
     port_pair;
       port_source 20–21;
     replace_tos 240 upc 1000000 upc_penalty drop;
   };
```

To change the destination IP address in the QoS IP frame condition list number 3 to 123.2.1 from 123.123.2.1-123.123.2.123

```
(config)# show qos-ip-list 3
  qos_ip_list 3 {
       ip_destination 123.123.2.1;
     replace_tos 240 upc 1000000 upc_penalty drop;
    };
(config)# qos-ip-list 3 –ip_destination 123.123.2.1
–123.123.2.123
(config)#  show qos-ip-list 3
  qos_ip_list 3 {
       ip_destination 123.123.2.1–123.123.2.123;
rlace_tos 240 upc 1000000 upc_penalty drop;
-};
(config)#
```

3. Show settings

   a. To display all the QoS IP frame condition list contents:

```
(config)# show qos-ip-list
    qos_ip_list 1 {
       protocol 6 ;
       tos 32 ;
       ip_pair ;
       ip_source 123.123.1.1 - 123.123.1.123 ;
       ip_destination 123.123.2.1 ;
       port_pair ;
       port_source 20 – 21 ;
       replace_tos 240 upc 1000000 upc_penalty drop ;
    } ;
    qos_ip_list 2 {
       protocol 1 ;
       tos 32 ;
       ip_pair ;
       ip_source 123.123.1.1 - 123.123.1.123 ;
       ip_destination 123.123.2.1 ;
       icmp_type 8 ;
       icmp_code 0 ;
       priority class 5 discard class 4 upc 5000000
upc_penalty modified
_priority_class 5 modified_discard_class 1 ;
    };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

b. To display optional QoS IP frame condition list:

```
(config)# show qos-ip-list 2
    qos_ip_list 2 {
       protocol 1 ;
       tos 32 ;
       ip_pair ;
       ip_source 123.123.1.1 - 123.123.1.123 ;
       ip_destination 123.123.2.1 ;
       icmp_type 8 ;
       icmp_code 0 ;
       priority class 5 discard class 2 upc 5000000
upc_penalty modified
_priority_class 3 modified_discard_class 1 ;
    } ;
(config)#
```

4. Delete settings:

   To delete the settings of QoS IP frame condition list number 2:

```
(config)# show qos-ip-list
    qos_ip_list 1;
    qos_ip_list 2;
    qos_ip_list 3;
(config)# delete qos-ip-list 2
(config)# show qos-ip-list
    qos_ip_list 1;
    qos_ip_list 3;
(config)#
```

5. Delete parameter:

   The transmission source IP address of QoS IP frame condition list number 1 is deleted.

   The qos-ip-list condition parameter that was set once can be deleted by delete command.

```
(config)#  show qos-ip-list 1
        qos_ip_list 1 {
                protocol 6;
                ip_pair_off;
                ip_source 123.123.1.1-123.123.1.123;
                ip_destination 123.123.2.1-123.123.2.123;
                port_pair_off;
                port_source 20-21;
                priority_class 2 discard_class 1;
        };
(config)#  delete qos-ip-list 1 -ip_source
(config)# show qos-ip-list 1
        qos_ip_list 1 {
                protocol 6;
                ip_pair_off;
                ip_destination 123.123.2.1-123.123.2.123;
                port_pair_off;
                port_source 20-21;
                priority_class 2 discard_class 1;
        };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Display of blank entry number:
   - Display of all blank entry numbers:

```
(config)#  show qos-ip-list free
Free number: 5,7,15-1024
(config)#
```

   - Display of first blank entry numbers:

```
(config)#  show qos-ip-list free
Free number: 5
(config)#
```

Related Commands

qos
qos-queue-list
qos-interface
qos-discard-mode
qos-ip-list-group
qos-tos-map
qos-ip

Related Information

For the flow control, refer to the *GR2000 Applications Guide*.

Precautions

1. The packets shown in the table below are distributed to each queue by fixed priority regardless of the flow control parameter set using this command. Replacing TOS is performed as a setting.

Table 1-97 Packet Type

Packet type	Output Priority*	Queuing Priority
The IP packet this device generated (rip etc.)	8	4
The ICMP packet this device generated	4	1
The IP packet this device relayed: (1) Packet with an option (IP header) (2) Fragmented packet (3) Redirected packet (4) ARP unresolved packet	4	4
ARP (ARP Request/ARP Response) packet this device generated	8	4
Layer 2 packet this device generated (WAN, ATM)	8	4
**: Output priority class refers to the queue number that loads the packet.*		

2. The QoS IP frame condition list used in the QoS frame condition group settings cannot be deleted.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

1.2.6 *qos-ip-list-group* (Information on QoS IP Frame Condition Group of the Old BSD UNIX-based Command System)

Establishes the QoS IP frame condition group settings. Combines QoS IP frame condition list which is defined in the QoS IP frame condition settings with the determination numbering. The maximum number of QoS IP frame condition groups that can be generated is 256 groups, and the maximum number of QoS IP frame condition lists which can be registered in a group is 1024.

Input Format

Setting information

```
[set] qos-ip-list-group <IP-List-Group Name> < IP List No. >
```

Adding settings

```
[set] qos-ip-list-group <IP-List-Group Name> < IP List No. >
```

Deleting settings

```
delete qos-ip-list-group <IP-List-Group Name> <IP List No.>
```

Displaying settings

```
show qos-ip-list-group [<IP-List-Group Name>]
```

Inserting settings

```
insert qos-ip-list-group <IP-List-Group Name> <Insert Position IP List
No.> <IP List No.>
```

Parameters

`<IP-List-Group Name>`

Description:	This parameter sets the name of the IP frame condition group
Default:	All groups displayed
Range of value:	Available characters are a maximum of 14 alphanumeric characters (first character must be alphabetic).

`<IP List No.>`

Description:	This parameter sets QoS IP frame condition list number. A maximum of 1024 lists can be registered. (Define the QoS IP frame condition list before entering this command.)
Default:	Deletion by a unit of designated group.
Range of value:	`1-1024`

`<Insert Position IP List No.>`

Description:	This parameter sets QoS IP frame condition list number in the inserting position. Inserts one before the designated condition list.
Default:	Cannot be omitted. Set QoS IP frame condition group number registered in QoS IP frame condition group being inserted.
Range of value:	`1-1024`

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Setting parameters:

   To set the QoS IP frame condition list number 3 in the QoS IP frame condition group named ip1:

```
(config)# qos -yes
(config)# qos-ip-list 3
(config)# qos-ip-list 18
(config)# qos-ip-list-group ip1 3
(config)# show qos-ip-list-group ip1
    qos_ip_list_group ip1 {
       ip_list 3;
    };
(config)#
```

2. Modifying parameters:

   To add the QoS IP frame condition list number 18 to the last list of the QoS IP frame condition group named ip1.

```
(config)# show qos-ip-list-group ip1
  qos_ip_list_group ip1 {
       ip_list 3;
  } ;
(config)# qos-ip-list-group ip1 18
(config)# show qos-ip-list-group ip1
    qos_ip_list_group ip1 {
     ip_list 3;
       ip_list 18;
  };
(config)#
```

3. Displaying settings:

   Displays the list's contents for the QoS IP frame condition group named ip1.

```
(config)# show qos-ip-list-group ip1
  qos_ip_list_group ip1 {
       ip_list 3;
     ip_list 18;
    };
(config)#
```

4. Inserting settings:

   To insert QoS IP frame condition list number 9 before list number 18 of the QoS IP frame condition group named ip1:

```
(config)# show qos-ip-list-group ip1
    qos_ip_list_group ip1 {
       ip_list 3;
       ip_list 18;
   };
(config)# insert qos-ip-list-group ip1 18 9
(config)# show qos-ip-list-group ip1
    qos_ip_list_group ip1 {
       ip_list 3;
       ip_list 9;
       ip_list 18;
    };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

5. Deleting settings:

   a. Deleting the list in the group

   To delete QoS IP frame condition list number 9 of the QoS IP frame condition group named ip1:

```
(config)# show qos-ip-list-group ip1
    qos_ip_list_group ip1 {
       ip_list 3;
       ip_list 9;
       ip_list 18;
    };
(config)# delete qos-ip-list-group ip1 9
(config)# show qos-ip-list-group ip1
    qos_ip_list_group ip1 {
       ip_list 3;
       ip_list 18;
    };
(config)#
```

   b. Deleting the group:

   To delete the QoS IP frame condition group named ip1:

```
(config)# delete qos-ip-list-group ip1
(config)#
```

Related Commands

qos-queue-list
qos-interface
qos-discard-mode
qos-ip-list
qos-tos-map
qos-ip

Related Information

For the flow control, refer to the *GR2000 Applications Guide*.

Precautions

1. The determination of QoS occurs in the order of the QoS IP frame condition list number designated in the QoS IP frame condition group.
2. QoS IP frame condition group cannot be deleted while in use with IP QoS settings.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.2.7 *qos-tos-map*

This command sets the TOS-QoS conversion table information. A maximum of eight entries (precedence) can be created.

Downloaded from www.Manualslib.com manuals search engine

The output priority and queuing priority are determined by a TOS value when parameters replace_tos and tos_map of QoS IP frame condition information or parameter replace_tos of filter list information are set.

The setting of this command is not required when the DSCP value of Diff-serv is associated with the output priority and queuing priority using the recommended value of this router. The recommended mapping list of the DSCP value and the output priority and queuing priority is shown in Table 1-99 Mapping Example of DSCP Value and Each Class.

Input Format

Settings

```
[set] qos-tos-map -precedence <No.> [-priority_class
<No.>][-discard_class <No.>]
```

Changing settings

```
[set] qos-tos-map -precedence <No.> [-priority_class
<No.>][-discard_class <No.>]
```

Deleting settings

```
delete qos-tos-map -precedence <No.>
```

Displaying settings

```
show qos-tos-map
```

Parameters

`-precedence <No.>`

Description: This parameter sets TOS precedence.

Default: See table below

Range of value: `0-7`

`-priority_class <No.>`

Description: This parameter sets the output priority class. In the case of output priority control, used as the output priority class. In the case of minimum bandwidth and round-robin, used as the queue number.

Default: See table below

Range of value: `1-8`

`-discard_class <No.>`

Description: This parameter sets the queuing priority class.

Default: See table below.

Range of value: `1-4`

Downloaded from www.Manualslib.com manuals search engine

Table 1-98 Initial Value Corresponding To TOS Value

Precedence	TOS Value	Output Priority Class	Queuing Priority Class
0	0-31	1	4
1	32-39	2	1
	40-47	2	4
	48-55	2	3
	56-63	2	2
2	64-71	3	1
	72-79	3	4
	80-87	3	3
	88-95	3	2
3	96-103	4	1
	104-111	4	4
	112-119	4	3
	120-127	4	2
4	128-135	5	1
	136-143	5	4
	144-151	5	3
	152-159	5	2
5	160-191	6	1
6	192-223	7	1
7	224-255	8	1

Downloaded from www.Manualslib.com manuals search engine

Table 1-99 Mapping of TOS Value and Output/Queuing Priority Class

Output/ Queuing Priority Class	Discard4	Discard3	Discard2	Discard1	
priority8					High
					priority
priority7					↑
priority6				101110	
				184	
priority5	100010	100100	100110		
	136	144	152		
priority4	011010	011100	011110		
	104	112	120		
priority3	010010	010100	010110		
	72	80	88		
priority2	001010	001100	001110		
	40	48	56		↓
priority1	000000				Low
	0				priority
Low drop ←				→ High drop	

Hatching part is RFC's recommended value.

Legend: DSCP value (Binary) / DSCP value (Decimal)

Hatched value is the RFC's recommended value:

- EF's recommended value
- Best Effort's recommended value
- AF's recommended value
- Random code point

Note: In output priority control, the packet with bigger priority is sent out by priority. In queuing priority, the one with smaller value is discarded by priority.

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Setting parameters

   To set the priority class 2 and queuing priority class in TOS precedence:

```
(config)# qos -yes
(config)# qos-tos-map -precedence 1 -priority_class 2
-discard_class 1
(config)# show qos-tos-map
    qos_tos_map {
        precedence 1 priority_class 2 discard_class 1 ;
    } ;
(config)#
```

2. Modifying parameters

   To change the queuing priority class in TOS precedence 1 from 1 to 2:

```
(config)# show qos-tos-map
    qos_tos_map {
        precedence 1 priority_class 2 discard_class 1 ;
    } ;
(config)# qos-tos-map -precedence 1 -discard_class 2
(config)#  show qos-tos-map
    qos_tos_map {
        precedence 1 priority_class 2 discard_class 2 ;
    } ;
(config)#
```

3. Showing settings

   To display content:

```
(config)# show qos-tos-map
    qos_tos_map {
        precedence 1 priority_class 2 discard_class 1 ;
        precedence 2 priority_class 3 discard_class 2 ;
    } ;
(config)#
```

4. Deleting settings

   To delete the settings of TOS precedence 1:

```
(config)# show qos-tos-map
    qos_tos_map {
        precedence 1 priority_class 2 discard_class 1 ;
        precedence 2 priority_class 3 discard_class 2 ;
    } ;
(config)# delete qos-tos-map -precedence 1
(config)#  show qos-tos-map
    qos_tos_map {
        precedence 2 priority_class 3 discard_class 2 ;
    } ;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

```
qos
qos-queue-list
qos-interface
qos-discard-mode
qos-ip-list
qos-ip-list-group
qos-ip
```

Related Information

For the flow control, refer to the *GR2000 Applications Guide*.

Precautions

1. Multiple IP frame condition groups cannot be set as inbound/outbound in a single interface.
2. When exp is specified as a flow detection condition parameter by qos-ip-list, only "in" specification is valid on the entry. "out" specification is invalid in this case. The entry is valid only on the core router in an MPLS network. It is invalid on the entrance and exit edge routers in an MPLS network.
3. Only the interface specification in RP after RP-C or RP-D is valid for the IP QoS information when exp is specified as a flow detection condition parameter by qos-ip-list or when replace-exp is specified as a flow control parameter. The interface specification in RP other than described above is invalid.
4. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.2.8 *qos-ip* (Information on IP QoS of the Old BSD UNIX-based Command System)

Establishes the IP QoS settings. The Qos IP frame condition group is determined against the interface defined in the IP or IP-address settings. When IP QoS settings are established, QoS is determined against the receipt packet or transmission packet in an applicable interface. A maximum of 512 entries can be generated per device (maximum interface 256, inbound/outbound for one interface).

Input Format

Settings

```
[set] qos-ip {<Line Name> | <DLCI Name> | <Group Name> |
<Timeslot Name> | <Peer Name> | <VC Name> }{ -in | -out }
-ip_list_group<qos-ip-list-group Name>
```

Change settings

```
[set] qos-ip {<Line Name> | <VPVC Name> | <DLCI Name> |
<Group Name> | <Timeslot Name> | <Peer Name> | <VC Name> }{ -in | -out }
-ip_list_group<qos-ip-list-group Name>
```

Delete settings

```
delete qos-ip {<Line Name> | <DLCI Name> | <Group Name> | <Timeslot Name>
| <Peer Name> | <VC Name> }{ -in | -out }
```


Downloaded from www.Manualslib.com manuals search engine

Display settings

```
show qos-ip [{<Line Name> | <VPVC Name> | <DLCI Name> | <Group Name>
| <Timeslot Name> | <Peer Name> | <VC Name> }]
```

Parameters

```
{ <Line Name> | <DLCI Name> | <Group Name> | <Timeslot Name> | <Peer Name> |
<VC Name> }
```

Description: Sets the name of the relevant interface established in IP or IP-address settings. (Before entering this command, establish IP or IP-address settings.)

Default: Cannot be omitted

```
{ -in | -out }
```

Description: Sets inbound/outbound. Set inbound, outbound, or both simultaneously for one interface.

in: Inbound (setting frame input side)

out: Outbound (setting frame output side)

Default: Cannot be omitted.

```
-ip_list_group <qos-ip-list-group Name>
```

Description: Sets QoS IP frame condition group names. (Before entering this command, establish the QoS IP frame condition group.)

Default: Cannot be omitted.

Examples

1. Setting parameters (settings are inbound)

   To set IP frame condition group named ip1 in the interface named office1:

```
(config)# line office1 ethernet 0/0
(config)# ip office1 170.10.10.10/24
(config)# qos yes
(config)# qos-ip-list 3
(config)# qos-ip-list-group ip1 3
(config)# qos-ip office1 -in -ip_list_group ip1
(config)# show qos-ip office1
  qos-ip office1 in ip_list_group ip1 ;
(config)#
```

2. Setting parameters (settings are inbound and outbound)

   To set the IP frame condition groups named ip1 and ip2 respectively in the interface designated inbound and outbound.

```
(config)# qos-ip office1 -in -ip_list_group ip1
(config)# qos-ip office1 -out -ip_list_group ip2
(config)# show qos-ip office1
    qos-ip office1 in ip_list_group ip1 ;
    qos-ip office1 out ip_list_group ip2 ;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Changing parameters

   To change IP frame condition group names from ip1 to ip3 in the interface named office1:

```
(config)# show qos-ip office1
    qos-ip office1 in ip_list_group ip1 ;
(config)# qos-ip office1 -in -ip_list_group ip3
(config)#  show qos-ip office1
    qos-ip office1 in ip_list_group ip3 ;
(config)#
```

4. Displaying settings

   To display the setting contents of the interface named office1:

```
(config)# show qos-ip ether1
    qos-ip office1 in ip_list_group ip3 ;
    qos-ip office1 out ip_list_group ip2 ;
(config)#
```

5. Deleting settings

   To delete inbound settings of the interface named office1:

```
(config)# show qos-ip office1
    qos-ip office1 in ip_list_group ip3;
    qos-ip office1 out ip_list_group ip2;
(config)# delete qos-ip office1 -in
(config)# show qos-ip office1
    qos-ip office1 out ip_list_group ip2;
(config)#
```

Related Commands

qos
qos-queue-list
qos-interface
qos-discard-mode
qos-ip-list
qos-ip-list-group
qos-tos-map
ip
ip-address

Related Information

For the flow control, refer to the *GR2000 Applications Guide*.

Precaution

1. Figure 1-12 shows the effect of QoS configuration definition output priority setting in ATM line. The output priority setting is valid in group name that grouped VC tokyo1 and Inbound (frame input side) of VC name tokyo2, but invalid in Outbound (frame output side) because ATM line does not control sending control. When output priority is set to Inbound of Ethernet, WAN, or ATM line, the setting is invalid at sending by ATM line. For example, when output priority is set in Inbound of line name tokyo4, it is valid at outputting packet received from the target line to line name tyokyo3 (WAN line), but invalid at outputting to tokyo1 or tokyo2 (ATM line).

Downloaded from www.Manualslib.com manuals search engine

2. When exp is specified as a flow detection condition parameter by qos-ip-list, the entry is enabled only on in designation. out designation is disabled. The entry is enabled only on the core router in an MPLS network. The entry and exit edge routers in an MPLS network are disabled.
3. When exp is specified as a flow detection condition parameter by qos-ip-list or -replace-exp is specified as a flow control parameter, only the interface designation in RP after RP-C or RP-D is enabled to the IP QoS information. The interface designation in RP except described above is disabled.
4. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

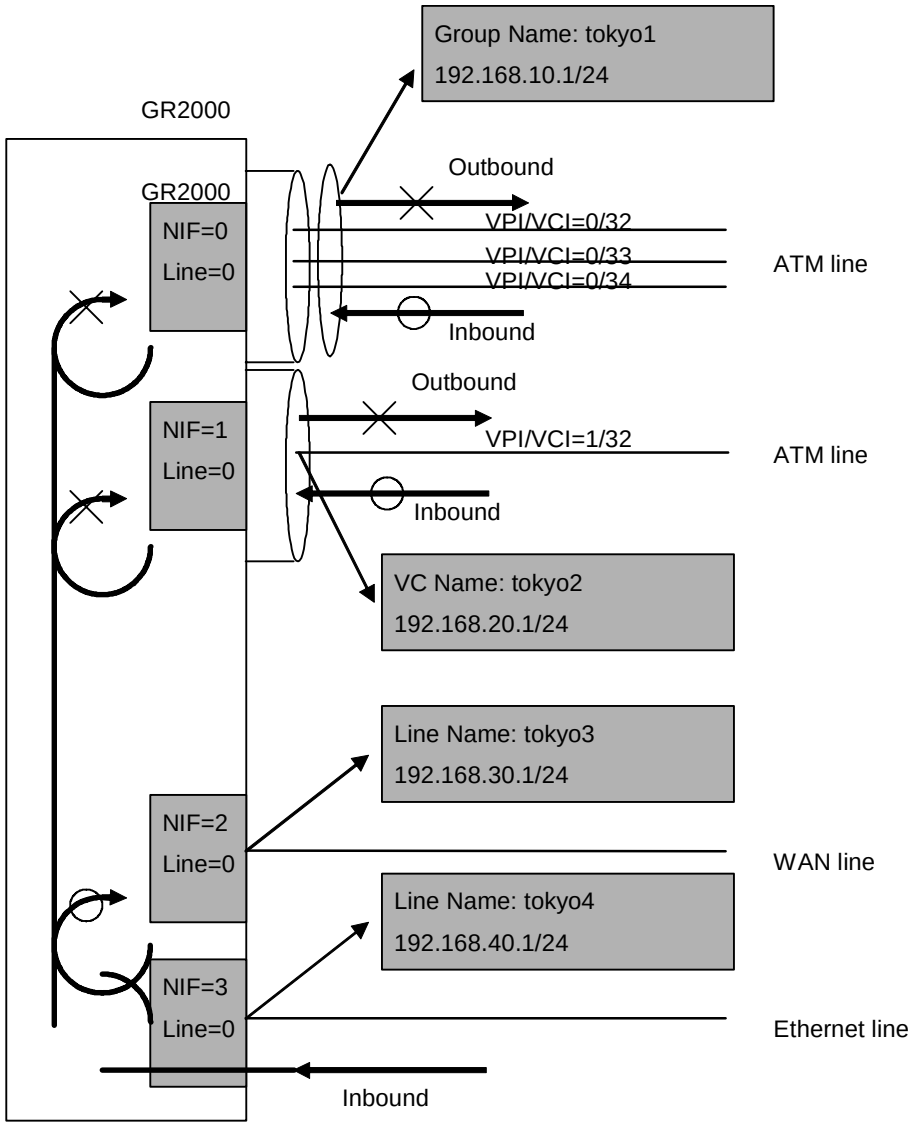


Figure 1-12 Effect of QoS Configuration Definition Output Priority in ATM Line

Downloaded from www.Manualslib.com manuals search engine

1.2.9 *qos-ipx*

Sets IPX QoS settings. A maximum of 160 entries can be generated per device.

Input Format

Settings

```
[set] qos-ipx {<Line Name> | <DLCI Name> | <VC Name> | <Group Name> |
<Timeslot Name> | <Peer Name> } [-priority_class <No.>],[-discard_class
<No.>]
```

Change settings

```
[set] qos-ipx {<Line Name> | <DLCI Name> | <VC Name> | <Group Name> |
<Timeslot Name> | <Peer Name> } [-priority_class <No.>],[-discard_class
<No.>]
```

Delete settings

```
delete qos-ipx {<Line Name> | <DLCI Name> | <VC Name> | <Group Name> |
<Timeslot Name> | <Peer Name> }
```

Display settings

```
show qos-ipx [{<Line Name> | <DLCI Name> | <VC Name> | <Group Name> |
<Timeslot Name> | <Peer Name> }]
```

Parameters

`{ <Line Name> | <DLCI Name> | <VC Name> | <Group Name> | <Timeslot Name> | <Peer Name> }`

Description: This parameter sets the relevant interface name established in the IPX routing interface settings. (Before entering this command, establish the IPX routing interface settings.)

Default: Cannot be omitted

`-priority_class <No.>`

Description: This parameter sets the output priority class. In the case of output priority control, used as output priority class. In the case of bandwidth and the round-robin, used as the queue number.

Default: `4`

Range of value: `1-8`

`-discard_class <No.>`

Description: This parameter sets the queuing priority class.

Default: `4`

Range of value: `1-4`

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Setting parameters:

   To set the output priority class 3 and the queuing priority class 1 in the interface named office1:

```
(config)# ipx -yes
(config)# ipx-interface office1
(config)# qos yes
(config)# qos-ipx office1 -priority_class 3
-discard_class 1
(config)# show qos-ipx
    qos_ipx office1 priority_class 3 discard_class 1 ;
(config)#
```

2. Modifying parameters:

   To change the queuing priority of the interface named office1 from 1 to 2:

```
(config)# show qos-ipx
show qos-ipx
    qos_ipx office1 priority_class 3 discard_class 1 ;
(config)# qos-ipx office1 -discard_class 2
(config)# show qos-ipx
    qos_ipx office1 priority_class 3 discard_class 2 ;
(config)#
```

3. Displaying settings:

   a. To display all:

```
(config)# show qos-ipx
    qos_ipx office1 priority_class 3 discard_class 2 ;
    qos_ipx office2 priority_class 4 discard_classe 2 ;
(config)#
```

   b. To display the name of the optional interface:

```
(config)# show qos-ipx office1
    qos_ipx office1 priority_class 3 discard_class 2 ;
(config)#
```

4. Deleting settings:

   To delete the settings of the interface named office1:

```
(config)# show qos-ipx
    qos_ipx office1 priority_class 3 discard_class 2 ;
    qos_ipx office2 priority_class 4 discard_class 2 ;
(config)# delete qos-ipx office1
(config)# show qos-ipx
    qos_ipx office2 priority_class 4 discard_class 2 ;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

5. Deleting parameters:

   To delete the discard-class of interface name office 1.

```
(config)# show qos-ipx
       qos_ipx office1 priority_class 3 discard_class 2 ;
(config)# delete qos-ipx office1 -discard_class
(config)# show qos-ipx
       qos_ipx office2 priority_class 4  ;
(config)#
```

Related Commands

qos
qos-queue-list
qos-interface
qos-discard-mode
ipx-interface

Precaution

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.2.10 *qos-bridge*

Sets the QoS settings. A maximum of 160 entries can be generated per device.

Input Format

Settings

```
[set] qos-bridge {<Line Name> | <DLCI Name> | <VC Name> |
<Group Name> | <Timeslot Name> | <Peer Name> }
[-priority_class <No.>],[-discard_class <No.>]
```

Change settings

```
[set] qos-bridge {<Line Name> | <DLCI Name> | <VC Name> |
<Group Name> | <Timeslot Name> | <Peer Name> }
[-priority_class <No.>],[-discard_class <No.>]
```

Delete settings

```
delete qos-bridge {<Line Name> | <DLCI Name> | <VC Name> |
<Group Name> | <Timeslot Name> | <Peer Name> }
```

Display settings

```
show qos-bridge [{<Line Name> | <DLCI Name> | <VC Name> |
<Group Name> | <Timeslot Name> | <Peer Name> ]
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

```
{ <Line Name> | <DLCI Name> | <VC Name> | <Group Name> |
<Timeslot Name> | <Peer Name> }
```

Description: This parameter sets the relevant interface name established in the bridge interface settings. (Before entering this command, establish the bridge interface settings.)

Default: Cannot be omitted.

-priority_class <No.>

Description: This parameter sets the output priority class. In the case of output priority control, used as the output priority class. In the case of bandwidth and round-robin, used as the queue number.

Default: 4

Range of value: 1-8

-discard_class <No.>

Description: This parameter sets the queuing priority class.

Default: 4

Range of value: 1-4

Examples

1. Setting parameters:

   To set the output priority class 3 and queuing priority class 1 in the interface named office1:

```
(config)# bridge-interface office1 -spt
(config)# qos -yes
(config)# qos-bridge office1 -priority_class 3
-discard_class 1
(config)# show qos-bridge
    qos_bridge office1 priority_class 3 discard_class 1 ;
(config)#
```

2. Modifying parameters:

   To change the queuing priority class of the interface named office1 from 1 to 2:

```
(config)# show qos-bridge
show qos-bridge
    qos_bridge office1 priority_class 3 discard_class 1 ;
(config)# qos-bridge office1 -discard_class 2
(config)# show qos-bridge
    qos_bridge office1 priority_class 3 discard_class 2 ;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Displaying settings:

   a. To display all:

```
(config)# show qos-bridge
    qos_bridge office1 priority_class 3 discard_class 2 ;
    qos_bridge office2 priority_class 4 discard_class 2 ;
(config)#
```

   b. To display the optional interface name:

```
(config)# show qos-bridge office1
    qos_bridge office1 priority_class 3 discard_class 2 ;
(config)#
```

4. Deleting settings:

   To delete the settings of the interface named office1.

```
(config)# show qos-bridge
    qos_bridge office1 priority_class 3 discard_class 2 ;
    qos_bridge office2 priority_class 4 discard_class 2 ;
(config)# delete qos-bridge office1
(config)# show qos-bridge
    qos_bridge office2 priority_class 4 discard_class 2 ;
(config)#
```

5. Deleting parameters:

   To delete the discard_class of interface name office 1.

```
(config)# show qos-bridge
      qos_bridge office1 priority_class 3 discard_class 2
;
(config)# delete qos-bridge office1 -discard_class
(config)# show qos-bridge
       qos_bridge office2 priority_class 4  ;
(config)#
```

Related Commands

```
qos
qos-queue-list
qos-interface
qos-discard-mode
bridge-interface
```

Precaution

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.2.11 *qos-hdlc-passthrough*

Establish HDLC passthrough QoS settings. A maximum of 160 entries can be generated per device.

Downloaded from www.Manualslib.com manuals search engine

Input Format

Settings

```
[set] qos-hdlc-passthrough {<Line Name> | <DLCI Name> | <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name> } [-priority_class <No.>]
[-discard_class <No.>]
```

Changing settings:

```
[set] qos-hdlc-passthrough {<Line Name> | <DLCI Name>| <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name> } [-priority_class <No.>
[-discard_class <No.>]
```

Deleting settings:

```
delete qos-hdlc-passthrough {<Line Name> | <DLCI Name>| <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name>}
```

Displaying settings:

```
show qos-hdlc-passthrough [{<Line Name> | <DLCI Name>| <VC Name> | <Group
Name> | <Timeslot Name> | <Peer Name>}]
```

Parameters

`{ <Line Name> | <DLCI Name>| <VC Name> | <Group Name> | <Timeslot Name> | <Peer Name> }`

Description: This parameter sets the relevant interface name established in the bridge interface settings. (Before entering this command, establish the bridge interface settings.) Only a WAN interface can be specified. The HDLC passthrough QoS information of LAN and ATM interfaces operates with the value set using qos-bridge.

Default: Cannot be omitted

`-priority_class <No.>`

Description: This parameter sets the output priority class. In the case of output priority control, used as the output priority class. In the case of bandwidth and round-robin, used as a queue number.

Default: `4`

Range of value: `1-8`

`-discard_class <No.>`

Description: This parameter sets the queuing priority class.

Default: `4`

Range of value: `1-4`

Downloaded from www.Manualslib.com manuals search engine

Examples

1. Setting parameters:

   To set the output priority class 3 and queuing priority class 1 in the interface named office1:

```
(config)# bridge-interface office1 -yes
(config)# qos -yes
(config)# qos-hdlc-passthrough office1 -priority_class 3 -discard_class 1
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office1 priority_class 3 discard_class 1;
(config)#
```

2. Modifying parameters:

   To change the queuing priority class of the interface named office1 from 1 to 2:

```
(config)# show qos-hdlc-passthrough
show qos-hdlc-passthrough
       qos_hdlc_passthrough office1 priority_class 3 discard_class 1;
(config)# qos-hdlc-passthrough office1 -discard_class 2
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office1 priority_class 3 discard_class 2;
(config)#
```

3. Displaying settings:

   a. To display all:

```
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office1 priority_class 3 discard_class 2;
       qos_hdlc_passthrough office2 priority_class 4 discard_class 2;
(config)#
```

   b. To display the optional interface name:

```
(config)# show qos-hdlc-passthrough office1
       qos_hdlc_passthrough office1 priority_class 3 discard_class 2;
(config)#
```

4. Deleting settings:

   To delete the settings of the interface named office1:

```
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office1 priority_class 3 discard_class 2;
       qos_hdlc_passthrough office2 priority_class 4 discard_class 2;
(config)# delete qos-hdlc-passthrough office1
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office2 priority_class 4 discard_class 2;
(config)#
```

5. Deleting parameters:

   To delete the settings of the interface named office1 discard class:

```
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office1 priority_class 3 discard_class 2 ;
(config)# delete qos-hdlc-passthrough office1 -discard_class
(config)# show qos-hdlc-passthrough
       qos_hdlc_passthrough office2 priority_class 4  ;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related commands

qos
qos-queue-list
qos-interface
qos-discard-mode
bridge-interface

Precaution

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

1.2.12 shaper (shaper transmission information)

This sets shaper transmission information. Three types of queuing modes, outbound priority control, low latency queuing + weighted fair queuing (LLQ+3WFQ) and weighted fair queuing (4WFQ), are set in interfaces. It is possible to produce a maximum of 256 entries per RP.

Input Format

Settings

```
[set] shaper {-set_default_user_priority|-set_default_user_priority_off}
[set] shaper rate_limited_queueing <VLAN_Name>
[[peak_rate {<kbit/s> | <Mbit/s>M}] {Setting the queuing mode}]
```

Setting the queuing mode

1. In the case of output priority control:
   ```
   priority [<Length1> [<Length2> [<Length3> [<Length4>]]]]
   ```
2. In the case of low latency queuing + weighted fair queuing (LLQ+3WFQ):
   ```
   llq+3wfq <Rate1>% [<Length1>] <Rate2>% [<Length2>]
   <Rate3>% [<Length3>]
   { 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% }
   [<Length4>]
   ```
3. In the case of weighted fair queuing (4WFQ):
   ```
   4wfq <Rate1>% [<Length1>] <Rate2>% [<Length2>]
   <Rate3>% [<Length3>] <Rate4>% [<Length4>]
   ```

Changing settings:

```
[set] shaper {-set_default_user_priority|-set_default_user_priority_off}
[set] shaper rate_limited_queueing <VLAN_Name>
[[peak_rate {<kbit/s> | <Mbit/s>M}] {Setting the queuing mode}]
```

Setting the queuing mode

1. In the case of output priority control:
   ```
   [priority] [<Length1> [<Length2> [<Length3> [<Length4>]]]]
   ```
2. In the case of low latency queuing + weighted fair queuing (LLQ+3WFQ):

Downloaded from www.Manualslib.com manuals search engine

- If the queuing mode is not omitted

```
llq+3wfq <Rate1>% [<Length1>] <Rate2>% [<Length2>]
<Rate3>% [<Length3>]
{ 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% }
[<Length4>]
```

- If the queuing mode is omitted

```
[<Rate1>% [<Length1>] [<Rate2>% [<Length2>]
[<Rate3>%[<Length3>]
[{ 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% }
[<Length4>]]]]]
```

3. In the case of weighted fair queuing (4WFQ):

- If the queuing mode is not omitted

```
4wfq <Rate1>% [<Length1>] <Rate2>% [<Length2>]
<Rate3>% [<Length3>] <Rate4>% [<Length4>]
```

- If the queuing mode is omitted

```
[<Rate1>% [<Length1>] [<Rate2>% [<Length2>]
[<Rate3>% [<Length3>] [<Rate4>% [<Length4>]]]]]
```

Deleting settings:

```
delete shaper [rate_limited_queueing <VLAN Name>]
delete shaper [-set_default_user_priority_off |
-set_default_user_priority]
```

Displaying settings:

```
show shaper [rate_limited_queueing <VLAN Name>]
```

Parameters

`[{ -set_default_user_priority | -set_defaulet_user_priority_off}]`

`-set_default_user_priority:`

Rewrites user priority in Tag-VLAN to default 0 and sends.

`-set_default_user_priority_off:`

Sends by the set user priority by the "flow qos" command

Default: -set_default_user_priority

Range of value: None

`rate_limited_queueing`

Sets fixed bandwidth

`<VLAN Name>`

Sets VLAN line name set by configuration definition

`peak_rate {<kbit/s> | <Mbit/s>M}`

Sets the maximum bandwidth

Description: None

Default: In the case of kbit/s is specified: 500 to 980000
In the case of Mbit/s is specified: 1M to 980M

Downloaded from www.Manualslib.com manuals search engine

```
priority [<Length1> [<Length2> [<Length3> [<Length4>]]]]
```

Sends packets from high priority queues. Packets are sent from lower priority queues only if there are no packets in higher priority queues. Table 1-100, Parameters of each queuing mode, gives a list of parameters for each queuing mode.

```
llq+3wfq <Rate1>% [<Length1>] <Rate2>% [<Length2>] <Rate3>% [<Length3>] { 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80%| 90% | 100% } [<Length4>]
```

If queue 4 is set as the minimum guaranteed bandwidth and it contains packets, the packets are sent unconditionally. Send information is output from queues 1 - 3 according to weight. Table 1-100, Parameters of each queuing mode, gives a list of parameters for each queuing mode.

```
4wfq <Rate1>% [<Length1>] <Rate2>% [<Length2>] <Rate3>% [<Length3>] <Rate4>% [<Length4>]
```

Send information is output from queues 1 - 4 according to the weight. Table 1-100, Parameters of each queuing mode, gives a list of parameters for each queuing mode.

Table 1-100 Parameters for each queuing mode

Item		Parameter	Supported specifications 1000BASE-SX 1000BASE-LX 1000BASE-LH NEB1G-2D	Description
Queue count		--	4 queue	--
Physical line maximum send bandwidth		--	986Mbit/s	--
Send bandwidth not subject to shaping		--	6Mbit/s	--
User priority rewrite in Tag-VLAN		-set_default_user_priority -set_default_user_priority_off		Sets rewrite of user priority in Tag-VLAN.
Traffic type		rate_limited_ququeing	Fixed bandwidth	Set when securing fixed bandwidth.
Interface name		<VLAN Name>		Sets name of interface specifying send control.
VLAN line maximum send bandwidth		peak_rate	500kbit/ to 980Mbit/s	Sets maximum send bandwidth of VLAN lines.
Output priority control	Queue mode	priority	Output priority control	Sets outbound priority control.
	Queue length	<Length>	0 to 4000(*1)	Sets queue length for each queue.
LLQ+3WFQ	Queue mode	llq+3wfq	LLQ+3WFQ	Sets low latency queuing + weighted fair queuing (LLQ+3WFQ).
	Minimum guaranteed bandwidth (low latency queuing)	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100%		Selects from 10%, 20%, 30%,40%,50%,60%,70%,80%,90% and 100% and sets.
	Maximum send bandwidth (weighted fair queuing)	<Rate>	1 to 100%	Sets maximum send bandwidth for each queue.
	Queue length	<Length>	0 to 4000(*1)	Set length of each queue.

Downloaded from www.Manualslib.com manuals search engine

Table 1-100 Parameters for each queuing mode

Item		Parameter	Supported specifications 1000BASE-SX 1000BASE-LX 1000BASE-LH NEB1G-2D	Description
4WFQ	Queue mode	4wfq	4WFQ	Sets weighted fair queuing (4WFQ).
	Maximum send bandwidth	<Rate>	1 to 100%	Sets maximum send bandwidth for each queue.
	Queue length	<Length>	0 to 4000(*1)	Set length of each queue
*(*1) If queue length is not set in each queue, default 0 is assigned. Table 1-101, Default length of each queue, indicates the default length of each queue.*				

Table 1-101 Default length of each queue

Queue number	Default queue length
1	400
2	300
3	250
4	200
It is possible to change the threshold at which discard begins in NE1G-2D in two stages. The discard threshold is set by the queue length of shaper send information. Correspondence between packet priority and discard threshold is indicated below. ** High priority packets (*1): Discard if queued packets exceed queue length* ** Low priority packets (*2): Discard if queued packets exceed one-half the queue length* *(*1): Packets in which 1 is the lowest bit of user priority* *(*2): Packets in which 0 is the lowest bit of user priority*	

Examples

1. Setting parameters:
   - Setting VLAN1 priority control in outbound priority control

```
(config)# shaper rate_limited_queueing VLAN1 peak_rate 20000 priority 800
600 400 200
(config)# show shaper rate_limited_queueing VLAN1
shaper {
   rate_limited_queueing {
            VLAN1 peak_rate 20000 priority 800 600 400 200;
   }
}
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Setting VLAN2 priority control in low latency queuing + weighted fair queuing (LLQ+3WFQ)

```
(config)# shaper rate_limited_queueing VLAN2 peak_rate 20000 llq+3wfq 1%
9% 40% 50%
(config)# show shaper rate_limited_queueing VLAN2
shaper {
   rate_limited_queueing {
           VLAN2 peak_rate 20000 llq+3wfq 1% 9% 40% 50%;
   }
}
(config)#
```

- Setting VLAN3 in weighted fair queuing (4WFQ)

```
(config)# shaper rate_limited_queueing VLAN3 peak_rate 20000 4wfq 1% 9%
40% 50%
(config)# show shaper rate_limited_queueing VLAN3
shaper {
   rate_limited_queueing {
           VLAN3 peak_rate 20000 4wfq 1% 9% 40% 50%;
   }
}
(config)#
```

2. Changing parameters:
   - Changing the maximum VLAN1 bandwidth to 30mbps

```
(config)# show shaper rate_limited_queueing VLAN1
shaper {
   rate_limited_queueing {
           VLAN1 peak_rate 20000 priority 800 600 400 200;
   }
}
(config)# shaper rate_limited_queueing VLAN1 peak_rate 30M
(config)# show shaper rate_limited_queueing VLAN1
shaper {
   rate_limited_queueing {
           VLAN1 peak_rate 30M priority 800 600 400 200;
   }
}
(config)#
```

3. Displaying setting information:
   - Displaying all information

```
(config)# show shaper
shaper {
   set_default_user_priority;
   rate_limited_queueing {
           VLAN1 peak_rate 30M priority 800 600 400 200;
           VLAN2 peak_rate 20000 llq+3wfq 1% 9% 90% 50%;
           VLAN3 peak_rate 20000 4wfq 1% 9% 40% 50%;
   }
}
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Displaying random VLAN line name settings

```
(config)# show shaper rate_limited_queueing VLAN2
shaper {
   rate_limited_queueing {
           VLAN2 peak_rate 20000 llq+3wfq 1% 9% 90% 50%;
   }
}
(config)#
```

4. Deleting setting information:
   - Deleting VLAN line name VLAN1 settings

```
(config)# show shaper
shaper {
   set_default_user_priority;
   rate_limited_queueing {
           VLAN1 peak_rate 30M priority 800 600 400 200;
           VLAN2 peak_rate 20000 llq+3wfq 1% 9% 90% 50%;
           VLAN3 peak_rate 20000 4wfq 1% 9% 40% 50%;
   }
}
(config)# delete shaper rate_limited_queueing VLAN1
(config)# show shaper
shaper {
   set_default_user_priority;
   rate_limited_queueing {
           VLAN2 peak_rate 20000 llq+3wfq 1% 9% 90% 50%;
           VLAN3 peak_rate 20000 4wfq 1% 9% 40% 50%;
   }
}
(config)#
```

Related commands

flow,flow filter,flow qos

Related information

None

Precaution

It may not be possible to guarantee the specified bandwidth if the flow control function is activated in gigabit Ethernet.

Downloaded from www.Manualslib.com manuals search engine

1.3 COPS

1.3.1 COPS

The configuration definition commands and parameters for defining the information that manages a cops command are described below. A security function is not used when an encryption key is not set using this command.

Input Format

Setting information

```
[set] cops [{-no | -yes}] -pepid <PEPID>
           -primary <IP-Address> [-primary_port <Port No.>]
           [-backup <IP-Address> [-backup_port <Port No.>]]
           [-server_password <keyid> <Password>
           [-cops_password1 <keyid> <Password>]
           [-cops_password2 <keyid> <Password>]
           [-cops_password3 <keyid> <Password>]
           [-cops_password4 <keyid> <Password>]
           [-cops_password5 <keyid> <Password>]]
           [-average_packet_size <packet size>]
           [-retry_time <retry time>]
```

Modifying information

```
[set] cops [{-no | -yes}] [-pepid <PEPID>]
           [-primary <IP-Address>]
           [-primary_port <Port No.>]
           [-backup <IP-Address>]
           [-backup_port <Port No.>]
           [-server_password <keyid> <Password>]
           [-cops_password1 <keyid> <Password>]
           [-cops_password2 <keyid> <Password>]
           [-cops_password3 <keyid> <Password>]
           [-cops_password4 <keyid> <Password>]
           [-cops_password5 <keyid> <Password>]
           [-average_packet_size <packet size>]
           [-retry_time <retry time>]
```

Displaying information

```
delete cops
```

Deleting information

```
show cops
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

`[{-no | -yes}]`

Description: This parameter specifies the use and disuse of a cops command.
-no: Not used.
-yes: Used.

Default: -no

Range of value: None

`-pepid <PEPID>`

Description: This parameter is an identification name in the primary server or backup server of this router. It is recommended to specify the IP-Address or host name of this router used.

Default: This parameter cannot be omitted.

Range of value: A character string exceeding one character and not exceeding 14 characters is set using double quotation marks (“). Alphanumeric characters and special characters can be entered. However, a character string can be entered without using double quotation marks (“) when no special character (e.g., space) is contained in an entry character string. However, notice that the characters below cannot be used. “(double quotation mark), { (beginning of brace), } (end of brace), ‘ (single quotation mark), ; (semicolon), $ (dollar), and ’ (reverse single quotation mark). For more information, see Table 2-1, in *GR2000 Configuration Commands, Vol. 1*.

Table 1-102 Allowable Characters

Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code
Space	0x20	0	0x30	@	0x40	P	0x50	---	---	p	0x70
!	0x21	1	0x31	A	0x41	Q	0x51	a	0x61	q	0x71
---	---	2	0x32	B	0x42	R	0x52	b	0x62	r	0x72
#	0x23	3	0x33	C	0x43	S	0x53	c	0x63	s	0x73
---	---	4	0x34	D	0x44	T	0x54	d	0x64	t	0x74
%	0x25	5	0x35	E	0x45	U	0x55	e	0x65	u	0x75
&	0x26	6	0x36	F	0x46	V	0x56	f	0x66	v	0x76
---	---	7	0x37	G	0x47	W	0x57	g	0x67	w	0x77
(	0x28	8	0x38	H	0x48	X	0x58	h	0x68	x	0x78
)	0x29	9	0x39	I	0x49	Y	0x59	i	0x69	y	0x79
*	0x2A	:	0x3A	J	0x4A	Z	0x5A	j	0x6A	z	0x7A
+	0x2B	---	---	K	0x4B	[	0x5B	k	0x6B	---	---
---	---	<	0x3C	L	0x4C	\	0x5C	l	0x6C	|	0x7C
-	0x2D	=	0x3D	M	0x4D	]	0x5D	m	0x6D	---	---
.	0x2E	>	0x3E	N	0x4E	^	0x5E	n	0x6E	~	0x7E
/	0x2F	?	0x3F	O	0x4F	_	0x5F	o	0x6F	---	---

Downloaded from www.Manualslib.com manuals search engine

-primary <IP-Address>

Description: This parameter sets the IP address of a primary server.

Default: This parameter cannot be omitted.

Range of value: IPv4 address (nnn.nnn.nnn.nnn): 0.0.0.0 to 255.255.255.255

[-primary_port <Port No.>]

Description: This parameter sets the port number of a primary server.

Default: 3101

Range of value: 0 to 65535 (decimal)

[-backup <IP-Address>]

Description: This parameter sets the IP address of a backup server.

Default: This parameter is set to non-specification.

Range of value: IPv4 address (nnn.nnn.nnn.nnn): 0.0.0.0 to 255.255.255.255

[-backup_port <Port No.>]

Description: This parameter sets the port number of a backup server.

Default: 3101

Range of value: 0 to 65535 (decimal)

[-server_password <keyid><Password>]

Description: This parameter sets the server password (encryption key). Set cops_password when setting this parameter.

Default: This parameter is set to non-specification.

Range of value: keyid: 1 to 2147483647 (7FFFFFFF)
A character string of a password exceeding one character and not exceeding 64 characters is set using double quotation marks (“). Alphanumeric characters and special characters can be entered. However, a character string can be entered without using double quotation marks (“) when no special character (e.g., space) is contained in an entry character string.
However, notice that the characters below cannot be used. “(double quotation mark), { (beginning of brace), } (end of brace), ‘ (single quotation mark), ; (semicolon), $ (dollar), and ’ (reverse single quotation mark). For more information, see Table 1-102

[-cops_password n <keyid><Password>](n indicates numbers 1 to 5.)

Description: This parameter sets the COPS password (encryption key). Set server_password when setting this parameter.

Default: This parameter is set to non-specification.

Range of value: keyid: 1 to 2147483647 (7FFFFFFF)
Set different values to five keyids, respectively.
A character string of a password exceeding one character and not exceeding 64 characters is set using double quotation

Downloaded from www.Manualslib.com manuals search engine

marks (“). Alphanumeric characters and special characters can be entered. However, a character string can be entered without using double quotation marks (“) when no special character (e.g., space) is contained in an entry character string.
However, notice that the characters below cannot be used. “(double quotation mark), { (beginning of brace), } (end of brace), ‘ (single quotation mark), ; (semicolon), $ (dollar), and ’ (reverse single quotation mark). For more information, see Table 1-102

`[-average_packet_size <packet size>]`

Description: This parameter specifies the average packet size.

Default: 1024 (bytes)

Range of value: 24 to 65535 (bytes)

`[-retry_time <retry time>]`

Description: This parameter specifies the number of retry times when the connection to the policy server fails. If reconnection to the policy server has failed as many times as the specified retry number, the policy information set to this device from the policy server is cleared.

Default: 3

Range of value: 0 to 10

Examples

1. Setting parameters:

   PEPID and the IP address of a primary server are set using a cops control function.

```
(config)#  cops -yes -pepid Tokyo1 -primary 10.10.11.5
(config)#  show cops
cops yes{
      pepid Tokyo1;
      primary 10.10.11.5;
};
(config)#
```

   PEPID, the IP address of a primary server, the port number of a primary server, the IP address of a backup server, the port number of a backup server, a server password, and a COPS password are set using a cops control function.

Downloaded from www.Manualslib.com manuals search engine

```
(config)#  cops -yes -pepid Tokyo1 -primary 10.10.11.5 -primary_port 50001
-backup 10.10.11.6 -backup_port 50002 -server_password abcdefg
-cops_password1 1 hijklmn
(config)#  show cops
cops yes{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50002;
      server_password 10 xxxxxxx;
      cops_password1 1 xxxxxxx;
};
(config)#
```

2. Changing parameters:

   A cops control function is changed to disuse.

```
(config)#  show cops
cops yes{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50002;
};
(config)#  cops -no
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50002;
};
(config)#
```

   The port number of a backup server is changed.

```
 (config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50002;
};
(config)#  cops -backup_port 50003
(config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50003;
};
(config)#
```

3. Displaying setting information:

   The contents of setting are displayed.

```
 (config)#  show cops
 cops no{
       pepid Tokyo1;
       primary 10.10.11.7 primary_port 50001;
 };
 (config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Deleting parameters:

   The definition of COPS is deleted.

```
(config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.7 primary_port 50001;
      backup 10.10.11.6 backup_port 50002;
};
(config)#  delete cops
(config)#  show cops
no cops entry.
(config)#
```

   The port number of a backup server is deleted.

```
(config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50003;
};
(config)#  cops --backup_port
(config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6
};
(config)#
```

   The IP address of a backup server is deleted.

   When the IP address is deleted, the port number is also deleted simultaneously.

```
(config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
      backup 10.10.11.6 backup_port 50003;
};
(config)#  cops --backup
(config)#  show cops
cops no{
      pepid Tokyo1;
      primary 10.10.11.5 primary_port 50001;
};
(config)#
```

Related Commands

flow

qos

qos-disard-mode

Downloaded from www.Manualslib.com manuals search engine

Precausion

1. -pepid and -primary cannot be deleted by specifying a parameter.
2. Before setting this command, set the flow entry reservation for cops using a flow cops_range command and then set qos cops. If not, this command cannot be set.
3. Set IP information to an interface. The interface information of this router is not displayed in a policy server even if cops is activated using this command with the IP information not set.
4. The information set in a policy server is deleted from this router when no is specified in COPS configuration definition or when COPS configuration definition is deleted.
5. flow cops_range (flow information for cops) cannot be changed when yes is specified in COPS configuration definition. Specify no in COPS configuration definition and then change flow cops_range.
6. flow cops_range cannot be deleted or qos cops cannot be changed and deleted when COPS configuration definition exists. Delete COPS configuration definition and then delete flow cops_range or change and delete qos cops.
7. If the parameter in this command has been changed while using COPS, re-connect with the policy server, and re-set the information set from this device's policy server.
8. The information set from the policy server in the changed interface is re-specified when qos-discard-mode (QoS discard mode) is changed while a COPS command is being used.
9. Adjust them to the setting of a policy server when setting -pepid, -server_password, and -cops_password parameters.
10. If setting and/or deletion of the policy has been made from the policy server to this device in the RM duplication configuration, RP may re-actuate if the system is altered.
11. It is not possible to delete the ip configuration defining information of the interface that has set the information from the policy server while COPS is in use. Delete the data from the policy server or deactivate the COPS configuration definition, and then delete the ip configuration definition.
12. When the COPS configuration defining information is changed or deleted, the statistical information of the show filter-flow and the show qos-ip-flow of all the interfaces with which the flow configuration definition is set, are cleared to zero. For the show-filter-flow and show qos ip-flow commands, refer to *GR2000 Operations Commands, Vol. 2*, show filter-flow and show qos ip-flow commands.
13. Confirm (using the ping command) that the communication route has been established between this device and the policy server before introducing cops yes.

Downloaded from www.Manualslib.com manuals search engine

Chapter 2
IPX/Bridge Information

2.1 IPX Objects

This section explains the configuration command and parameters that define IPX routing protocol information.

2.1.1 *ipx*

This sets the operation information for IPX routing.

Input Format

Setting information

```
[set] ipx [{ -no | -yes }]  [-watchdog_spoofing_interval <Minute>]
[-watchdog_forwarding_interval <Minute>]
```

Change settings

```
[set] ipx [{ -no | -yes }]  [-watchdog_spoofing_interval <Minute>]
[-watchdog_forwarding_interval <Minute>]
```

Display settings

```
show ipx
```

Delete settings

```
delete ipx
```

Parameters

`-no | -yes`

Description: This parameter determines whether the IPX routing in this device will be valid (yes) or invalid (no). This device does not execute the IPX routing operation when this setting is invalid.

Default: `-no`

`-watchdog_spoofing_interval <Minute>`

Description: This parameter specifies the watchdog packet that confirms the server connection for the client of another network via this router, and also specifies the time interval (minutes) for this router to carry out the spoofing response.

Default: `60`

Range of value: `1-1440`

Downloaded from www.Manualslib.com manuals search engine

```
-watchdog_forwarding_interval <Minute>
```

Description: This parameter specifies the time interval (minutes) for forwarding the watchdog packet without spoofing.

Default: 20

Range of value: 1-1440

Examples

1. Setting parameters

   To set the IPX routing operation to Enable and set the timing of the watchdog spoofing response and forwarding intervals:

```
(config)# ipx -yes -watchdog_spoofing_interval 10
-watchdog_forwarding_interval 4
(config)#
```

2. Change parameters

   To change the IPX routing operation to Disable:

```
 (config)# ipx -no
 (config)#
```

3. Display settings

   To display the content of the definition:

```
(config)# show ipx
ipx yes {
    watchdog_spoofing_interval 10 ;
    watchdog_forwarding_interval 15;
} ;
(config)#
```

4. Delete settings

```
(config)# delete ipx
(config)#
```

5. Delete parameter

   To delete the watchdog-spoofing-interval.

```
(config)# show ipx
ipx yes {
    watchdog_spoofing_interval 10 ;
    watchdog_forwarding_interval 15;
} ;
(config)# delete ipx -watchdog_spoofing_interval
(config)# show ipx
ipx yes {
    watchdog_forwarding_interval 15;
} ;
```

Related Commands

None

Downloaded from www.Manualslib.com manuals search engine

2.1.2 *ipx-interface*

This sets the interface information for the IPX routing protocol.

Input Format

Setting information

```
[set]ipx-interface {<Line Name>|<DLCI  Name> |<VC Name> | <Peer Name> |
<Timeslot Name>
     |  <Group Name> }
     [-watchdog_spoofing { periodic | proxy | forward }]
     [{ -serialization_filtering_off | -serialization_filtering }]
     [{ -diagnostic_packet_forwarding | -diagnostic_packet_forwarding_off
     }]
     [{ -non_periodic_rip_send_off | -non_periodic_rip_send }]
     [{ -non_periodic_sap_send_off | -non_periodic_sap_send }]
     [-periodic_rip_interval <Minute>]
     [-periodic_sap_interval <Minute>]
     [{ -nearest_sap_reply | -nearest_sap_reply_off }]
     {ethernet802_3_network_address <IPX Address>
     ethernet2_network_address <IPX Address>llc_network_address <IPX
     Address>   snap_network_address <IPX Address> | network_address <IPX
     Address>   -node_address <MAC Address>}
```

Changing information

```
[set] ipx-interface { <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name>
| <Timeslot Name> | <Group Name>
     }
     [-watchdog_spoofing { periodic | proxy | forward }]
     [{ -serialization_filtering_off | -serialization_filtering}]
     [{ -diagnostic_packet_forwarding | -diagnostic_packet_forwarding_off
     }]
     [{ -non_periodic_rip_send_off | -non_periodic_rip_send }]
     [{ -non_periodic_sap_send_off | -non_periodic_sap_send }]
     [-periodic_rip_interval <Minute>]  [-periodic_sap_interval <Minute>]
     [{ -nearest_sap_reply | -nearest_sap_reply_off }]
     [{ethernet802_3_network_address <IPX Address>
     ethernet2_network_address <IPX Address> llc_network_address <IPX
     Address>   snap_network_address <IPX Address> | network_address <IPX
     Address> -node_address <MAC Address>}]
```

Delete settings

```
delete ipx-interface {<Line Name> | <DLCI  Name> | <VC Name> | <Peer Name>
| <Timeslot Name> | <Group Name>}
```

Display settings

```
show ipx-interface [{ <Line Name> | <DLCI Name> | <VC Name> | <Peer Name>
| <Timeslot Name> | <Group Name> }]
```

Parameters

```
{ <Line Name> | <DLCI  Name> |<VC Name> | <Peer Name> | <Timeslot Name> |
<Group Name> }
```

Description: This parameter specifies the interface name to be set. Pay attention to the followings.

Downloaded from www.Manualslib.com manuals search engine

- IPX routing interface can be defined only to the interface that is set IP interface (except rmEthernet, AUX, tunnel. Therefore, IPX interface alone cannot be defined.

- Up to 160 per system and up to 32 per RP can be defined. This value is the IPX network count. For example, when 4 types of frames are set in Ethernet, consider that 4 interfaces are used. In WAN or ATM, only 1 interface is used.

- When the specified interface is ATM, WAN frame relay, or ISDN, ipx-arp setting is required. (When this setting is omitted, uni-cast communication is not available.)

- In case of WAN frame relay, set ipx_outgoing option by dlci command to the DLCI under the target frame relay. If not, IPX packet is not relayed.

- In case of broadcast type ISDN, stop the sending of cycle RIP/SAP and define the necessary RIP/SAP information by static.

Default: None (cannot be omitted)

`-watchdog_spoofing { periodic | proxy | forward }`

Description: This parameter is the watchdog packet's spoofing response function switch. You can configure up to 160 per system and 32 per RP. Select from the following options:

`periodic:` Carry out the spoofing response (cycle)

`proxy:` Unconditionally carry out the spoofing response

`forward:` Do not carry out the spoofing response

Default: Periodic

`{ -serialization_filtering_off | -serialization_filtering }`

Description: This parameter is the filter function switch when the serialization packet is received.

`serialization_filtering_off`
(Do not discard the serialization packet.)

`serialization_filtering`
(Discard the serialization packet.)

Default: `-serialization_filtering`

`{ -diagnostic_packet_forwarding | -diagnostic_packet_forwarding_off }`

Description: This parameter is the forwarding switch when the diagnostic packet is received.

`diagnostic_packet_forwarding_off`
(Do not forward diagnostic packet.)

`diagnostic_packet_forwarding`
(Forward diagnostic packet.)

Default: `-diagnostic_packet_forwarding_off`

Downloaded from www.Manualslib.com manuals search engine

{ -non_periodic_rip_send_off | -non_periodic_rip_send }

Description: This parameter is the RIP packet's send switch when there is a change in the network where the RIP Request reply and the local router can be routed at start-up.

non_periodic_rip_send_off
(Do not send RIP packet.)

non_periodic_rip_send
(Send RIP packet.)

Default: -non_periodic_rip_send

{ -non_periodic_sap_send_off | -non_periodic_sap_send }

Description: This parameter is the SAP packet's send switch when there is a change in the server by which the SAP Request and the local router can be routed at start-up.

non_periodic_sap_send_off
(Do not send SAP packet.)

non_periodic_sap_send
(Send SAP packet.)

Default: -non_periodic_sap_send

-periodic_rip_interval <Minute>

Description: This parameter specifies the send interval (minutes) of the periodic RIP packet.

Default: 1

Range of value: 0-1440 (0 does not deliver this packet periodically)

-periodic_sap_interval <Minute>

Description: This parameter specifies the send interval (minutes) of the periodic SAP packet.

Default: 1

Range of value: 0-1440 (0 does not deliver this packet periodically

{ -nearest_sap_reply | -nearest_sap_reply_off }

Description: This parameter sets the operation of the nearest SAP for the relevant interface. The following operations may be executed.

nearest_sap_reply :
Reply to the nearest SAP request even when this interface already has the SAP information for the service type with the nearest SAP request. However, the reply information does not contain the SAP information learned by the nearest SAP request receive interface.

nearest_sap_reply_off :
Do not reply to the nearest SAP request when this interface already has the SAP information for the service type with the nearest SAP request.

Default: -nearest_sap_reply_off

Downloaded from www.Manualslib.com manuals search engine

`ethernet802_3_network_address <IPX Address>`

Description: This parameter specifies the network address in an 8-digit hexadecimal number used by the Ethernet interface according to the IEEE802.3 standard. It is only valid when the relevant interface is Ethernet.

`<IPX Address>`: Specify the pertinent network address.

Default: None

Range of value: `1-0xfffffffe` in `<IPX Address>`

`ethernet2_network_address <IPX Address>`

Description: This parameter specifies the network address used by the interface according to the standard of Ethernet V2.0, in an 8-digit hexadecimal number. It is only valid when the relevant interface is Ethernet.

`<IPX Address>`: Specify the pertinent network address.

Default: None

Range of value: `1-0xfffffffe in <IPX Address>`

`llc_network_address <IPX Address>`

Description: This parameter specifies the network address used with LLC in an 8-digit hexadecimal number. It is only valid when the relevant interface is Ethernet.

`<IPX Address>`: Specify the pertinent network address.

Default: None

Range of value: `1-0xfffffffe`

`snap_network_address <IPX Address>`

Description: This parameter specifies the network address used with SNAP in an 8-digit hexadecimal number. It is only valid when the relevant interface is Ethernet.

`<IPX Address>`: Specify the pertinent network address.

Default: None

Range of value: `1-0xfffffffe`

`network_address <IPX Address>`

Description: This parameter specifies the network address assigned to this interface in an 8-digit hexadecimal number only when the relevant interface is WAN or ATM.

`<IPX Address>`: Specify the pertinent network address.

Default: None

Range of value: `1-0xfffffffe`

Downloaded from www.Manualslib.com manuals search engine

-node_address <MAC Address>

Description: This parameter specifies the node address (MAC address) assigned to this interface in a 12-digit hexadecimal number only when the relevant interface is WAN or ATM.

Default: None

range of value: 00:00:00:00:00:01-ff:ff:ff:ff:ff:fe

Examples

1. Setting parameters:

   To set the interface information for Ethernet to all four frame types:

```
(config)# ipx-interface Department1 -watchdog_spoofing periodic
-serialization_filtering -diagnostic_packet_forwarding
-non_periodic_rip_send -non_periodic_sap_send
-periodic_rip_interval 1 -periodic_sap_interval 1
-nearest_sap_reply_ethernet802_3_network_address 11111111
ethernet2_network_address 22222222 llc_network_address 33333333
snap_network_address 44444444
```

   Setting of interface for WAN (PPP):

```
(config)# ipx-interface TokyoNagoya  network_address 33333333
node_address 33:22:22:22:22:11
(config)#
```

   Setting of interface for ATM or WAN (FR or ISDN)(when the interface is <DLCI Name>, <VC Name>, or <Peer Name>):

```
(config)# ipx-interface TokyoOsaka  network_address 33333333
node_address 33:22:22:22:22:11
(config)# ipx-arp 00:11:22:33:44:55 TokyoOsaka
```

   Setting of interface for ATM or WAN (FR)(when the interface is <Group Name>)

```
(config)# ipx-interface GROUP1  network_address 33333333 ¥
node_address 33:22:22:22:22:11
(config)# ipx-arp 00:11:22:00:00:01  TokyoOsaka
(config)# ipx-arp 00:11:22:00:00:03  TokyoKyoto
         :
(config)# ipx-arp 00:11:22:00:00:44  TokyoNgoya
```

   ipx-arp is set to DLCI, Peer, or VC controlled under an interface.

2. Changing parameters:

   To change the interface of WanLine1 to the watchdog spoofing response:

```
(config)# ipx-interfacer WanLine1 -watchdog_spoofing proxy
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Displaying settings:

   a. To display all:

```
(config)# show ipx-interface
ipx- interface EthNetLine1 {
    watchdog_spoofing proxy ;
    serialization_filtering ;
    diagnostic_packet_forwarding ;
    non_periodic_rip_send ;
    non_periodic_sap_send ;
    periodic_rip_interval 1 ;
    periodic_sap_interval 1 ;
    nearest_sap_reply ;
    ethernet802_3_network_address 11111111  ;
    ethernet2_network_address 22222222  ;
    llc_network_address 33333333  ;
    snap_network_address 44444444
} ;
ipx-interface WanLine1  {
    watchdog_spoofing periodic ;
    serialization_filtering ;
    diagnostic_packet_forwarding ;
    non_periodic_rip_send ;
    non-periodic_sap_send ;
    periodic_rip_interval 1 ;
    periodic_sap_interval 1 ;
    nearest_sap_reply ;
    network_address 33333333  ;
    node_address 33:22:22:22:22:11 ;
} ;
(config)#
```

   b. To display options:

```
(config)# show ipx- interface EthNetLine1
ipx- interface EthNetLine1 {
    watchdog_spoofing proxy ;
    serialization_filtering ;
    diagnostic_packet_forwarding ;
    non_periodic_rip_send ;
    non_periodic_sap_send ;
    periodic_rip_interval 1 ;
    periodic_sap_interval 1 ;
    nearest_sap_reply ;
    ethernet802_3_network_address 11111111  ;
    ethernet2_network_address 22222222  ;
    llc_network_address 33333333 ;
    snap_network_address 44444444
} ;
(config)#
```

4. Deleting settings:

   To delete the IPX interface information in the EthNetLine1 interface:

```
(config)# delete ipx-interface EthNetLine1
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

5. Deleting parameter:

   To delete the llc_network_address information of interface Department1.

```
(config)# show ipx-interface Department1
ipx-interface Department1 {
    ethernet802_3_network_address 11111111  ;
    ethernet2_network_address 22222222  ;
    llc_network_address 33333333 ;
};
(config)# delete ipx-interface Department1 -llc_network_address
config show ipx-interface Department1
ipx-interface Department1 {
    ethernet802_3_network_address 11111111  ;
    ethernet2_network_address 22222222  ;
}
```

Related Commands

line
ipx

Precaution

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

2.1.3 *ipx-arp*

This sets the ARP information when WAN (Frame Relay) is used.

Input Format

Setting information

```
[set] ipx-arp <MAC Address> {<DLCI  Name> | <VC Name> | <Peer Name> }
```

Change settings

```
[set] ipx-arp <MAC Address> {<DLCI  Name> | <VC Name> | <Peer Name>}
```

Delete settings

```
delete ipx-arp <MAC Address>
```

Display settings

```
show ipx-arp
```

Parameters

<MAC Address>

Description: This specifies the node address (MAC address).

Default: Cannot be omitted

Range of value: 00:00:00:00:00:01-ff:ff:ff:ff:ff:fe

Downloaded from www.Manualslib.com manuals search engine

```
{<DLCI  Name> | <VC Name> | <Peer Name> }
```

Description: This specifies the DLCI name for Frame Relay, or VC name for ATM.

Default: Cannot be omitted

Examples

1. Setting parameters

   To set vpvc2 to MAC address to 11:11:11:11:11:11 and dlci2 to 12:11:11:11:11:11, for WAN-FR:

```
(config)# ipx-arp 12:11:11:11:11:11 dlci2
(config)#
```

2. Changing parameters

   To change the ARP entry MAC address 11:11:11:11:11:11 to vpvc1:

```
(config)# ipx-arp 11:11:11:11:11:11 vpvc1
(config)#
```

3. Displaying settings

   To display all ARP table information:

```
(config)# show ipx-arp
ipx-arp {
11:11:11:11:11:11 vpvc1 ;
12:11:11:11:11:11 dlci2;
};
(config)#
```

4. Deleting settings

   To delete an ARP entry of MAC address 12:11:11:11:11:11:

```
(config)# delete ipx-arp 12:11:11:11:11:11
(config)#
```

Related Commands

ipx
ipx-interface
dlci
vc

Precautions

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

2.1.4 static-route

This command allows setting of the IPX static route.

Input Format

Setting information

```
[set] static-route destination_network <IPX Address>  next_hop_network
     <IPX Address>   next_hop_host <MAC Address>  hops <Hops>  ticks
     <Ticks>
```

Change settings

```
[set] static-route <No.> [destination_network <IPX Address>]
     [next_hop_network <IPXAddress>] [next_hop_host <MAC Address>] [hops
     <Hops>] [ticks <Ticks>]
```

Insert settings

```
insert static-route <No.> destination_network <IPX Address>
     next_hop_network <IPXAddress> next_hop_host <MAC Address> hops
     <Hops> ticks <Ticks>
```

Delete settings

```
delete static-route <No.>
```

Display settings

```
show static-route [<No.>]
```

Parameters

`destination_network <IPX  Address>`

Description: This parameter specifies the destination network address of the registered static routing entry.

Default: Cannot be omitted

Range of value: `1-0xfffffffe`

`next_hop_network <IPXAddress>`

Description: This parameter specifies the next network address for the forwarding destination of the IPX packet attached to the relevant destination address.

Default: Cannot be omitted

Range of value: `1-0xfffffffe`

`next_hop_host <MAC Address>`

Description: This parameter specifies the next host address for the forwarding destination of the IPX packet attached to the relevant destination address.

Default: Cannot be omitted

Range of value: `00:00:00:00:00:01-ff:ff:ff:ff:ff:fe`

Downloaded from www.Manualslib.com manuals search engine

hops <Hops>

Description: This parameter specifies the number of hops to the destination network.

Default: Cannot be omitted

Range of value: 1-15

ticks <Ticks>

Description: This parameter specifies the time required to send the packet to the destination network based on the number of ticks. Among the routes to the destination network, the one with the smallest number of ticks has priority.

Default: Cannot be omitted

Range of value: 1-65535

Examples

1. Setting parameters:

   To set the static routing to next hop network 22222222, next host address 02:11:11:11:11:11, and 1 hop, one tick for destination network address 11111111:

```
(config)# static-route destination_network 11111111
next_hop_network 22222222 next_hop_host 02:11:11:11:11:11
hops 1 ticks 1
(config)#
```

2. Changing parameters

   To change the number of hops to 2 and the number of ticks to 10 for static route entry number 2:

```
(config)# static-route 2 hops 2 ticks 10
(config)#
```

3. Inserting parameters

   To insert a new entry just before the entry:

```
(config)# insert static-route 1 destination_network 11111119
next_hop_network
22222229 next_hop_host 02:11:11:11:11:19 hops 1 ticks 1
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Displaying settings
   a. To display all:

```
(config)# show static-route
No.
----
        static-route {
   1         destination_network 21111111
             next_hop_network 12222222
             next_hop_host 02:21:11:11:11:11
             hops 1
             ticks 1 ;
   2         destination_network 11111111
             next_hop_network 22222222
             next_hop_host 02:11:11:11:11:11
             hops 2
             ticks 10;
     };
(config)#
```

   b. To display options for static route entry number 1:

```
(config)# show static-route 1
No.
----
        static-route {
   1         destination_network 21111111
             next_hop_network 12222222
             next_hop_host 02:21:11:11:11:11
             hops 1
             ticks 1 ;
        };
(config)#
```

5. Deleting settings
   a. To delete entry number 1:

```
(config)# delete static-route 1
(config)#
```

Related Commands

ipx
ipx interface

Precausion

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

2.1.5 static-sap

This command sets the static SAP information.

Input Format

Setting information

```
[set] static-sap server_name <Name>  type <Type>  hops <Hops>
     network_address <IPX Address>  [-node_address <MAC Address>]
     [-socket_number <Socket Number>] next_hop_network <IPX Address>
     next_hop_router_address <MAC Address>
```

Change settings

```
[set] static-sap <No.> [server_name <Name>]  [type <Type>]  [hops <Hops>]
     [network_address <IPX Address>] [-node_address <MAC Address>]
     [-socket_number <Socket Number>] [next_hop_network <IPX Address>]
     [next_hop_router_address <MAC Address>]
```

Insert settings

```
insert static-sap <No.> server_name <Name> type <Type> hops <Hops>
     network_address <IPX Address> [-node_address <MAC Address>]
     [-socket_number <Socket Number>] next_hop_network <IPX Address>
     next_hop_router_address <MAC Address>
```

Delete settings

```
delete static-sap <No.>
```

Display settings

```
show static-sap  [<No.>]
```

Parameters

`server_name <Name>`

Description: This parameter specifies the registered static server name.

Default: Cannot be omitted

Range of value: Maximum of 47 characters.

`type <Type>`

Description: This parameter specifies the service type (4-digit hexadecimal number). The reference values are shown in Table 2-1 below.

Downloaded from www.Manualslib.com manuals search engine

Table 2-1 Server Type Reference Values

Type	Server Type	Type	Server Type	Type	Server Type
0001	User	0021	NAS/SNA gateway	004d	Xtree network version
0002	User group	0023	NACS	0050	Btrieve VAP 411*1
0003	Print list	0024	Remote bridge server	0053	Print list user
0004	Novell file server	0026	Bridge server	0072	WAN copy utility
0005	Job server	0027	RCP/IP gateway	007a	TES NetWare for VWS*2
0006	Gateway1	0029	Gateway2	0098	NetWare access server
0007	Print server	002d	Time synchronization server	009e	PORLIST NetWare
0008	Archive list	002e	Archive server SAP	0107	NetWare386
0009	Archive server	0047	Advertising print server	0130	Communication executive
000a	Job list	004b	Btrieve VAP 50*1	0133	NSS domain
000b	Administration	004c	SQL VAP*1	0137	NetWare386 print list

**1: VAP = Value Added Process (component of NetWare286 software)*
**2: VMS = Virtual Memory System (DEC minicomputer operating system)*

Default: Cannot be omitted

Range of value: 4-digit hexadecimal number

`hops <Hops>`

Description: This parameter specifies the number of hops to the destination network.

Default: Cannot be omitted

Range of value: `1-15`

`network_address <IPX Address>`

Description: This parameter specifies the network address where the server exists.

Default: Cannot be omitted

Range of value: `1-0xfffffffe`

`-node_address <MAC Address>`

Description: This parameter specifies the node address of the server (MAC address.)

Default: `0x00-00-00-00-00-01`

Range of value: `00:00:00:00:00:01-ff:ff:ff:ff:ff:fe`

`-socket_number <Socket Number>`

Description: This parameter specifies a 4-digit hexadecimal socket number allocated to the service by which the client can make a request of the server.

Default: `0x0451`

Range of value: `0-0xfffe`

Downloaded from www.Manualslib.com manuals search engine

`next_hop_network <IPXAddress>`

Description: This parameter specifies the next network address for the forwarding destination of the packet to be sent to the server.

Default: Cannot be omitted

Range of value: `1-0xfffffffe`

`next_hop_router_address <MAC Address>`

Description: This parameter specifies the next router address (MAC address) for the forwarding destination of the packet to be sent to the server.

Default: Cannot be omitted

Range of value: `00:00:00:00:00:01-ff:ff:ff:ff:ff:fe`

Examples

1. Setting parameters:

   To set static SAP information on the server named server_x:

```
(config)# static-sap server_name server_x type 0011 hops 1
network_address 33333333 -node_address 02:22:22:22:22:22:22
next_hop_network 44444444 next_hop_router_address
02:33:33:33:33:33
(config)#
```

2. Changing parameters:

   To change only the type and the number of hops for SAP entry number 2:

```
(config)#  static-sap 2 type 0021 hops 2
(config)#
```

3. Inserting parameters:

   To insert static SAP information on server_y:

```
(config)# insert static-sap  1 server_name server_y type 0011
hops 1 network_address 33333333 -node_address 02:22:22:22:22:22
next_hop_network 44444444 next_hop_router_address
02:33:33:33:33:33
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

4. Displaying settings

   a. To display all:

```
(config)# show static-sap
No.
----
       static-sap {
   1       server_name server_x
           type 0011
           hops 1
           network_address 13333333
           node_address 02:22:22:22:22:22:55
           next_hop_network 34444444
           next_hop_router_address 12:33:33:33:33:33
   2       server_name aaaa
           type 0021
           hops 2
           network_address 33333333
           node_address 02:22:22:22:22:22:22
           next_hop_network 44444444
           next_hop_router_address 02:33:33:33:33:33
       } ;
(config)#
```

   b. To display options for SAP entry number 1:

```
(config)# show static-sap 1
No.
----
       static-sap {
   1       server_name server_x
           type 0011
           hops 1
           network_address 13333333
           node_address 02:22:22:22:22:22:55
           next_hop_network 34444444
           next_hop_router_address 12:33:33:33:33:33
       } ;
(config)#
```

5. Deleting settings

   To delete SAP entry number 1:

```
(config)# delete static-sap 1
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Deleting parameter

   The node_address of SAP information in No. 1 are deleted.

```
(config)# show static-sap 1
      sap {
          server_name server_x;
          type 0011;
          hops 1;
          network_address 13333333;
          node_address 02:22:22:22:22:22:55;
          next_hop_network 34444444;
          next_hop_router_address 12:33:33:33:33:33;
       } ;
(config)# delete static-sap 1 -node_address
config show  static-sap 1
       sap {
         server_name server_x;
          type 0011;
          hops 1;
          network_address 13333333;
          next_hop_network 34444444;
          next_hop_router_address 12:33:33:33:33:33;
       } ;
(config)#
```

Related Commands

ipx
ipx interface

Precautions

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

2.1.6 *rip-filtering*

This command filters a RIP packet. Filtering can be applied on the input or output ports.

Input Format

Setting information

```
[set] rip-filtering [-network <IPX Address>]
     [-port_network <IPX Address>] [{ -forward | -drop }]
     [{ -output | -input }]
```

Changing settings

```
[set] rip-filtering <No.> [-network <IPX Address>]
     [-port_network <IPX Address>]
     [{ -forward | -drop }]  [{ -output | -input }]
```


Downloaded from www.Manualslib.com manuals search engine

Inserting settings

```
insert rip-filtering <No.> [-network <IPX Address>]
     [-port_network <IPX Address>][{ -forward | -drop }]
     [{ -output | -input }]
```

Deleting settings

```
delete rip-filtering <No.>
```

Displaying settings

```
show rip-filtering [<No.>]
```

Parameters

`-network <IPX Address>`

Description: This parameter specifies the relevant network address. 0xffffffff specifies an all f's network broadcast.

Default: 0xffffffff

range of value: 0-0xffffffff

`-port_network <IPX Address>`

Description: This parameter specifies the interface to be filtered by its network address. 0xffffffff specifies an all f's network broadcast.

Default: 0xffffffff

Range of value: 0-0xffffffff

`{ -forward | -drop }`

Description: This parameter specifies the filtering operation. forward: RIP is forwarded. drop: RIP is dropped.

Default: forward

`{ -output | -input }`

Description: This parameter specifies the filtering mode. output: Specifies filtering to be applied when transmitting packets. input: Specifies filtering to be applied when receiving packets.

Default: output

Examples

1. Setting parameters

   To drop the RIP packet with network address 11111111 with a target interface in network address 22222222:.

```
(config)# rip_filtering -network 11111111 -port_network
22222222 -drop -output
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Changing parameters

   To change the operation of RIP filtering entry number 2 to drop and input:

```
(config)# rip_filtering  2 -drop -input
(config)#
```

3. Displaying settings

   a. To display all:

```
(config)# show rip_filtering
No.
----
       rip_filtering {
   1      filter network 11111111
          port_network 22222222
          forward
          output ;
   2      filter network 11111111
          port_network 22222222
          drop
          input ;
       };
(config)#
```

   b. To display options for RIP filtering entry number 1:

```
(config)# show rip_filtering 1
No.
----
       rip_filtering {
   1      filter network 11111111
          port_network 22222222
          forward
          output ;
       };
(config)#
```

4. Deleting settings

   To delete RIP filtering information entry number 1:

```
(config)# delete rip_filtering 1
(config)#

<5>Insertion of parameter
Insert a new entry just before the entry.

(config)# insert rip_filtering 1 -network 11111111
-port_network 22222222 -d\
drop -output
(config)#
```

5. Inserting parameter

   To insert the new entry in front of entry number1.

```
(config)# insert rip-filtering 1 -network 11111111 -port_network 22222222
-d¥
rop -output
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Deleting parameter

   The filtering operation and mode of SAP filtering information in No. 1 are deleted.

```
(config)# show rip-filtering 1
       filter {
          network 11111111;
          port_network 22222222;
          forward;
          output ;
       };
(config)# delete rip-filtering 1 -forward
(config)# delete rip-filtering 1 -output
(config)# show rip-filtering 1
       filtering {
          network 11111111;
          port_network 22222222;
       };
(config)#
```

Related Commands

ipx
ipx-interface

Precautions

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

2.1.7 *sap-filtering*

This command filters a SAP packet by setting the SAP filtering information. Filtering can be applied on the input on output ports.

Input Format

Setting information

```
[set] sap-filtering [-type <Type>] [-server_network <IPX Address>]
      [-port_network <IPX Address>] [{ -forward | -drop }]
      [{ -output | -input }]
```

Changing settings

```
[set] sap-filtering <No.> [-type <Type>]
      [-server_network <IPX Address>] [-port_network <IPX Address>]
      [{  -forward | -drop }]
      [{ -output | -input }]
```

Inserting settings

```
insert sap-filtering <No.> [-type <Type>]
      [-server_network <IPX Address>] [-port_network <IPX Address>]
      [{ -forward | -drop }]  [{ -output | -input }]
```


Downloaded from www.Manualslib.com manuals search engine

Deleting settings

```
delete sap-filtering <No.>
```

Displaying settings

```
show sap-filtering [<No.>]
```

Parameters

`-type <Type>`

Description: This parameter specifies the service type of the server to be filtered using a 4-digit hexadecimal number.

Default: `0xffff`

Range of value: `0-0xffff`

`-server_network<IPX Address>`

Description: This parameter specifies the network address of the destination server for the SAP packet to be filtered. `0xffffffff` specifies all interfaces.

Default: `0xffffffff`

Range of value: `0-0xffffffff`

`-port_network <IPX Address>`

Description: This parameter specifies the interface to be filtered by its network address. 0xffffffff specifies all interfaces.

Default: `0xffffffff`

Range of value: `0-0xffffffff`

`{ -forward | -drop }`

Description: This parameter specifies the filtering operation. `forward`: SAP is forwarded. `drop`: SAP is dropped.

Default: `forward`

`{ -output | -input }`

Description: This parameter specifies the filtering mode. `output`: specifies filtering to be applied to transmitting packets. `input`: specifies filtering to be applied to receiving packets.

Default: `output`

Examples

1. Setting parameters

   To forward the SAP information for server network address `11111111` and service type `1111` destined for network address `22222222`:

```
(config)# sap_filtering -type 1111 -server_network 11111111
-port_network 22222222
-forward -output
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Changing parameters

   To change the operation of SAP filtering information entry number 1 to drop and input:

```
(config)# sap_filtering  1 -drop -input
(config)#
```

3. Inserting parameters

   To insert new information:

```
(config)# insert sap_filtering 1 -type 1111 -server_network
11111111 -port_network
22222222 -forward -output
(config)#
```

4. Displaying settings

   a. To display all:

```
(config)# show sap_filtering
No.
----
       sap_filtering {
   1      filter type 2111
          server_network 21111111
          port_network 12222222
          forward
          output ;
   2      filter type 1111
          server_network 11111111
          port_network 22222222
                :
       };
(config)#
```

   b. To display options for SAP filtering information entry number 1:

```
(config)# show sap_filtering 1
No.
----
       sap_filtering {
   1      filter type 2111
          server_network 11111111
          port_network 22222222
          forward
          output ;
     };
(config)#
```

5. Deleting settings

   To delete SAP filtering information entry number 1:

```
(config)# delete sap_filtering 1
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Deleting parameter

   The filtering operation and mode of SAP filtering information in No. 1 are deleted.

```
(config)# show sap-filtering 1
    filter {
          type 2111;
          server_network 11111111;
          port_network 22222222;
          forward;
          output ;
     };
(config)# delete sap-filtering 1 -forward
(config)# delete sap-filtering 1 -output
(config)# show sap-filtering 1
    filter {
          type 2111;
          server_network 11111111;
          port_network 22222222;
    };
(config)#
```

Related Commands

ipx
ipx-interface

Precautions

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

2.1.8 *ipx-filtering*

This command filters an IPX packet by setting the IPX filtering information. Filtering is done before the IPX packet is transmitted.

Input Format

Setting information

```
[set] ipx-filtering { <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name>

      | <Timeslot Name > | <Group Name> } { -forward | -drop }
protocol_type
      <Number>  network <IPX Address>  socket <Socket> [-netmask <Mask>]
      destination_network <IPX Address>  destination_socket <Socket>
      [-destination_netmask <Mask>]
```


Downloaded from www.Manualslib.com manuals search engine

Changing settings

```
[set] ipx-filtering <No.> [{ <Line Name> | <DLCI  Name> |
      <VC Name> | <Peer Name> | <Timeslot Name> | <Group Name>}]
      [{ -forward | -drop }]  [protocol_type <Number>]
      [network <IPX Address>] [socket <Socket>] [-netmask <Mask>]
      [destination_network <IPX Address>]
      [destination_socket <Socket>]
      [-destination_netmask <Mask>]
```

Inserting settings

```
insert ipx-filtering <No.> { <Line Name> | <DLCI  Name> |
      <VC Name> | <Peer Name> | <Timeslot Name> | <Group Name> }
      { -forward | -drop }  protocol_type <Number>
      network <IPX Address> socket <Socket> [-netmask <Mask>]
      destination_network <IPX Address>
      destination_socket <Socket>
      [-destination_netmask <Mask>]
```

Deleting settings

```
delete ipx-filtering <No.>
```

Displaying settings

```
show ipx-filtering [<No.>]
```

Parameters

`{ <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name> | <Timeslot Name> | <Group Name> }`

Description: This parameter specifies the interface name to be set.

Default: `Cannot be omitted`

`{ forward | drop }`

Description: This parameter specifies the filtering operation. `forward`: Packet is forwarded. `drop`: Packet is dropped.

Default: `forward`

`-protocol_type <Number>`

Description: This parameter specifies the type of protocol to be filtered using a 2-digit hexadecimal number.

Default: `Cannot be omitted.`

Range of value: `0-0xff`

`network <IPX Address>`

Description: This parameter specifies the IPX network address to be filtered.

Default: `Cannot be omitted`

Range of value: `0-0xffffffff`

`socket <Socket>`

Description: This parameter specifies the IPX socket number to be filtered using a 4-digit hexadecimal number.

Downloaded from www.Manualslib.com manuals search engine

Default: Cannot be omitted

Range of value: 0-0xffff

-netmask <Mask>

Description: This parameter specifies the range of subnets to be filtered by applying subnet masks.

Default: 0x00000000

Range of value: 0-0xffffffff

destination_network <IPX Address>

Description: This parameter specifies the network address for the destination of the IPX packet to be filtered.

Default: Cannot be omitted

Range of value: 0-0xffffffff

destination_socket <Socket>

Description: This parameter specifies the socket number for the destination of the IPX packet to be filtered using a 4-digit hexadecimal number.

Default: Cannot be omitted

range of value: 0-0xffff

-destination_netmask <Mask>

Description: This parameter specifies the reference mask value for specifying comparative ranges of the network addresses in the destination of the IPX packet when filtering.

Default: 0x00000000

Range of value: 0-0xffffffff

Examples

1. Setting parameters

   To suppress (drop) filtering of the IPX frame in interface line1:

```
(config)# ipx-filtering line1 drop protocol_type 06 network 32111111
socket 2221 -netmask ffffffff destination_network 43333333
destination_socket 2233  -destination_network ffffffff
(config)#
```

2. Changing parameters

   To change the operation of IPX filtering entry number 2 to forward and the protocol_type to 07:

```
(config)# ipx-filtering 2  forward protocol_type 07
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Displaying settings

   a. To display all:

```
(config)# show ipx-filtering
No.
    ipx-filtering {
   1        line1
            filter drop ;
            protocol_type 06
            network 32211111
            socket 2222
            netmask ffffffff
            destination_network 44333333
            destination_socket 2333
            destination_network ffffffff ;
   2        line2
            filter forward ;
            protocol_type 07
            network 32111111
            socket 2221
            netmask ffffffff
            destination_network 43333333
            destination_socket 2233
            destination_network ffffffff ;
        };
```

   b. To display options for IPX filtering entry number 1:

```
(config)# show ipx-filtering 1
No.
----
     ipx-filtering {
   1     line1
         filter drop ;
         protocol_type 06
         network 32211111
         socket 2222
         netmask ffffffff
         destination_network 44333333
         destination_socket 2333
         destination_network ffffffff ;
       };
(config)#
```

4. Deleting settings

   To delete IPX filtering entry number 1:

```
(config)# delete ipx-filtering 1
(config)#
```

5. Inserting parameters

   To insert new information:

```
(config)# insert ipx-filtering 1 line1 drop protocol_type 06 network
32111111 socket
2221 -netmask ffffffff destination_network 43333333 destination_socket
2233  -destination_network ffffffff
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

6. Deleting parameters

   To delete the netmask of IPX filtering number1.

```
(config)# delete ipx-filter 1 -network
(config)#
```

Related Commands

ipx
ipx-interface

Precausion

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

2.2 Bridge Objects

This section explains the configuration commands and parameters that define bridge information.

2.2.1 *bridge*

Function

Object for display of the Bridge information.

Input Format

```
show bridge
```

Example

```
(config)# show bridgee
bridge {
    bridge-interface line1 spt  {
                :
    } ;
    filtering-database aging 300 {
                :
           } ;
    extended-filtering yes {
      sk1 drop {
              type1 ctl value1 1 mask1 20 length1 1 offset1 0 ;
      } ;
    } ;
    spanning-tree {
                :
    } ;
} ;
(config)#
```

Related Commands

None

Precausion

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

2.2.2 *bridge-interface*

You can define the bridge interface configuration.

Input Format

Defining

```
[set] bridge-interface { <Line Name> | <DLCI  Name> |
     <VC Name> | <Peer Name> | <Group Name> | <Timeslot Name>}
     [{ -no | -yes | -spt }] [-cost <Cost>] [-priority <Priority>]
     [{ -disable | -enable }]
     [{ -translation | -translation_off }]
```

Modifying

```
[set] bridge-interface { <Line Name> | <DLCI  Name> |
     <VC Name> | <Peer Name> | <Group Name>  | <Timeslot Name>}
     [{ -no | -yes | -spt }]  [-cost <Cost>]
     [-priority <Priority>] [{ -disable | -enable }]
     [{ -translation | -translation_off }]
```

Deleting

```
delete bridge-interface { <Line Name> | <DLCI  Name> |
     <VC Name> | <Peer Name> | <Group Name> }
```

Displaying

```
show bridge-interface [{ <Line Name> | <DLCI  Name> |
     <VC Name> | <Peer Name> | <Group Name> }]
```

Parameters

```
{ <Line Name> | <DLCI Name> | <VC Name> | <Peer Name> | <Group Name> |
<Timeslot Name> }
```

Description: Specify the interface name. You must set the IP interface before configuring bridge. The maximum number is up to 160 per system and 32 per RP. In case of Frame Relay, you cannot use <timeslot> <groupname>. In case of ISDN, you can use <Peer Name> and cannot use <Group Name>. In case of ATM, you can use <VC Name> and <Group Name> that are specified to IP interface.

Default: None (cannot be omitted)

```
{  -no | -yes | -spt }
```

Description: You can define the bridge operation mode of the selected interface. Select one of the following.

no: Bridge function does not operate.

yes: Bridge function operates, but spanning-tree protocol does not.

spt: Bridge function and spanning-tree protocol operate.

Default: no

Downloaded from www.Manualslib.com manuals search engine

`-cost <Cost>`

Description: You can assign a cost parameter to calculate best path from each interface to the root bridge. This parameter determines which bridge interface offers a lower-cost path to the root bridge. This parameter is valid only for interfaces with Spanning Tree turned “on”.

Default: `10`

Range of value: `1-65535`

`-priority <Priority>`

Description: You can define the upper 8 bits of port ID (16 bits). Use port ID to decide which interface should do the Frame Relay when two or more interfaces on the same bridge are connected to the same network.

Default: `128`

Range of value `0-255`

`-disable | -enable`

Description: You can define whether the transition state of the relevant interface is active or not. With `-disable`, you can prohibit Frame Relay of the specified frame. This parameter is valid only for interfaces with bridge mode operational (`-spt`).

Default: `-enable`

`-translation | -translation_off`

Description: You can select the function to translate FDDI frame into the ether frame format when transmitting to WAN or ATM. This parameter is valid only when the specified interface is WAN or ATM. This parameter supports only the bridge, connected with the specified ether interface. Use it if you cannot recognize FDDI frame.

The translation of frame format described here is only for MAC header (regularized with IEEE802.1H), which does not support partitioning a frame (fragmentation) in the bridge.

-translation_off indicates no translation; -translation indicates translation.

Default: `-translation_off`

Examples

1. Parameter configuration

   To set the interface sk1 as a spanning-tree bridge interface:

```
(config)# bridge-interface line1 -spt -cost 10 -priority 128 -translation
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Parameter modification

   To modify the interface sk1 to the bridge interface, which does not allow spanning-tree operation, and the path cost to 20:

```
(config)# bridge-interface line1 -yes -cost 20
(config)#
```

3. Configuration display

   a. To display all:

```
(config)# bridge-interface
bridge-interface line2 spt {
    cost 10 ;
    priority 128 ;
    disable ;
    translation ;
} ;
bridge-interface line1 yes {
    cost 20 ;
    priority 128 ;
    translation ;
} ;
(config)#
```

   b. To display specific information:

```
(config)# bridge-interface line2
bridge-interface line2 spt {
    cost 10 ;
    priority 128 ;
    disable ;
    translation ;
} ;
(config)#
```

4. Configuration deletion

   To delete the bridge-interface of interface sk2:

```
(config)# delete bridge-interface line2
(config)#
```

5. Deleting parameters

   Interface name: To delete the cost or priority of bridge-interface of TokyoNagoya.

```
(config)# show bridge-interface TokyoNagoya
bridge-interface TokyoNagoya spt {
    cost 10 ;
    priority 128 ;
    disable ;
    translation ;
} ;
(config)# delete bridge-interface TokyoNagoya -cost
(config)# delete bridge-interface TokyoNagoya -priority
(config)# show bridge-interface TokyoNagoya
bridge-interface TokyoNagoya spt {
    disable ;
    translation ;
} ;
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

bridge
line

Precautions

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

2.2.3 *filtering-database*

By using filtering-database (FDB), you can delete and relay the frame, based on the source and destination MAC addresses. You can set the aging timer value and static entry.

Input Format

Defining

```
[set] filtering-database [ageing <Second>] <MAC Address>
     { drop | forward }  {<Line Name> | <DLCI  Name>  | <VC Name> |
     <Peer Name> | <Group Name> | <Timeslot>}
```

Modifying

```
[set] filtering-database [ageing <Second>] <No.> [<MAC Address>]
     [{ drop | forward }]  [{<Line Name> | <DLCI  Name> |
     <VC Name> | <Peer Name> | <Group Name> | <Timeslot>}]
```

Inserting

```
insert filtering-database  <No.> <MAC Address>
     { drop | forward }  {<Line Name> | <DLCI  Name> | <VC Name> |
     <Peer Name> | <Group Name> | <Timeslot>}
```

Deleting

```
delete filtering-database  <No.>
```

Displaying

```
show filtering-database
```

Parameters

`-ageing <Second>`

Description:	This parameter sets the age-out timer for dynamic entries in the filtering database.
Default:	300
Range of value	10-1000000

Downloaded from www.Manualslib.com manuals search engine

<MAC Address>

Description: Sets the static entry MAC address to register with the filtering-database in canonical representation.

Default: Cannot be omitted

Range of value Set MAC address to 48 bits.

drop | forward

Description: This sets filtering: drop deletes all frame destinations of the specified MAC address, and forward relays the frame destination from the specified MAC address to the indicated interface address. It also deletes the frame when receiving the specified frame from the indicated interface.

Default: Cannot be omitted

<Line Name> | <DLCI Name> | <VC Name> | <Peer Name> | <Group Name> | <Timeslot>

Description: Indicate the interface you selected for forwarding during filtering. The DLCI name can be specified for Frame Relay, and the VC name and group name can be specified for ATM. The Peer Name can be specified for ISDN.

Default: Cannot be omitted

Examples

1. Parameter configuration

   To set the aging of the filtering-database to 300 seconds, and the static entry for the MAC address to 11:22:33:11:11:11:

```
(config)# filtering-database -ageing 300 11:22:33:11:11:11 forward eth00
line1
(config)#
```

2. Parameter modification

   To change operation of the number 2 filtering-database entry to drop:

```
(config)# filtering-database 2  drop
(config)#
```

3. Configuration display

```
(config)# show filtering-database
  No.
----  filtering-database aging 300 {
   1      line2 11:22:33:12:11:11 drop ;
   2      line1 11:22:33:11:11:11 forward ;
     };
(config)#
```

4. Configuration deletion

   To delete the filtering-database information's second entry:

```
(config)# delete filtering-database 2
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

bridge
bridge-interface
line

Precaution

1. The value specified for ageing is ageing out within the range of the value that rounded out by 10 seconds unit. For example, when 30 to 39 is specified, ageing out in 40 seconds.
2. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

2.2.4 *extended-filtering*

You can set extended-filtering information to delete and relay the frame, based on bit pattern of the specific field designated by the MAC or data link header. Also you can use the BIT pattern of the arbitrary frame field.

You can set a maximum of three filtering entries. The parameter fields are the same in all three entries.

Input Format

Defining

```
[set] extended-filtering [{ yes | no }]
     { <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name> | <Group Name>
| <Timeslot>
     | all }  { drop | forward }  [{filter1 | filter2 | filter3 } { off |
     da | sa | dsap | ssap | ctl | oui | pid | type | user }] [-value
     <Value>] [-mask <Mask>]  [-length <Length>]  [-offset <Offset>]
```

Modifying

```
[set] extended-filtering  [{ yes | no }]<No.>
     [{ <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name> | <Group
Name> | <Timeslot>
     | all }]  [{ drop | forward }]  [{filter1 | filter2 | filter3 } { off
     | da | sa | dsap | ssap | ctl | oui | pid | type | user }] [-value
     <Value>] [-mask <Mask>]  [-length <Length>]  [-offset <Offset>]
```

Inserting

```
insert extended-filtering <No.>
     { <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name> | <Group Name>
| <Timeslot>
     | all }  { drop | forward }  [{filter1 | filter2 | filter3 } { off
     | da | sa | dsap | ssap | ctl | oui | pid | type | user }] [-value
     <Value>]  [-mask <Mask>]  [-length <Length>]  [-offset <Offset>]
```

Deleting

```
delete extended-filtering <No.>
```


Downloaded from www.Manualslib.com manuals search engine

Displaying

```
show extended-filtering [<No.>]
```

Parameters

```
{ -yes | -no }
```

Description: This parameter sets whether you perform extended-filtering: -yes indicates extended filtering, and no indicates -no extended filtering.

Default: -no

```
{ <Line Name> | <DLCI  Name> | <VC Name> | <Peer Name> | <Group Name> |
<Timeslot> | all }
```

Description: This parameter specifies the name of the interface that performs extended-filtering. When you specify all, all interfaces perform extended filtering. The DLCI name can be specified for Frame Relay, and the VC name and group name can be specified for ATM. The Peer Name can be specified for ISDN.

Default: Cannot be omitted

```
{ -drop | -forward }
```

Description: This parameter configures filtering operation: drop discards frames that match the filtering conditions, and forward relays frames that match the filtering conditions only to recipients specified by interface name.

Default: -drop

```
filter1-3 { off | da | sa | dsap | ssap | ctl | oui | pid | type | user }
```

Description: Specifies filtering conditions (choose from the list below). You can configure up to three items; however, only one item can be set at a time. For example, when configuring three items, first configure as filter1, then as filter2 and filter3.

off: No information

da: Recipient MAC address (6 octet)

sa: Sender MAC address (6 octet)

dsap: Recipient SAP (1 octet)

ssap: Sender SAP (1 octet)

ctl: Control field (1 octet)

oui: Organization code (3 octet)

pid: Protocol ID (2 octet)

type: Type field when the format is Ethernet.

user: Specifying any user defined fields.

Default: off

Downloaded from www.Manualslib.com manuals search engine

`-value <Value>`

Description: This parameter configures bit patterns (hexadecimal) that check filtering.

Default: `0`

Range of value: `0-0xfffffffffff`

`-mask <Mask>`

Description: Configures bit patterns (hexadecimal) that check filtering.

Default: `0`

Range of value: `0-0xfffffffffff`

`-length <Length>`

Description: Configures data length (octet number) of the field that checks filtering. This is valid only when chosen type is user.

Default: This parameter cannot be omitted when the user is specified by filter1 to 3.

Range of value: `1-6`

`-offset <Offset>`

Description: Configures offset value of the field that checks filtering. Offset value is expressed by setting recipient MAC address's first octet to `0`. When the frame is Ethernet or IEEE802.3, the recipient MAC address's first octet matches the first octet of the MAC header. When the frame is FDDI, the first MAC header octet is FC field, so you have to set the first MAC address octet following FC field to `0`. This is valid only when chosen type is user.

Default: `0`

Range of value: `0-56`

Examples

1. Setting parameters

   To set extended filtering (yes) for user defined fields as filtering to filter1 against interface sk3:

```
(config)# extended-filtering yes line3 drop filter1 user -value 30 -mask F0
-length\
 1 -offset 0
(config)#
```

2. Changing parameters

   To change extended filtering number 2 entry information to forward and the value to 10:

```
(config)# extended-filtering 2 forward filter1 -value 10
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Displaying setting information:

   a. Display all information:

```
(config)# extended-filtering
No.
----  extended-filtering yes {
 1         line1 drop {
                   filter1 ctl value 1 mask 20 length 1 offset 0 ;
           } ;
 2         line3 forward {
                   filter1 user value 10 mask 0 length 1 offset 0 ;
           } ;
    } ;
(config)#
```

   b. Displaying specific information:

```
(config)# show extended-filtering 1
 line drop {
         filter1 ct1 value 1 mask 20 length 1 offset 0 ;
} ;
(config)#
```

4. Deleting setting information

   To delete entry information number 1:

```
(config)# delete extended-filtering 1
(config)#
```

5. Deleting parameters:

   To delete the offset of entry information number1.

```
(config)# show extended-filtering 1
 Department1 drop {
         filter1 user value 000000000001 mask fffffffffff length 1 offset
0 ;
} ;
(config)#  delete extended-filtering 1 filter1 -offset
(config)# show extended-filtering 1
 Department1 drop {
          filter1 user value 000000000001 mask fffffffffff length 1 ;
} ;
```

Related Commands

bridge
bridge-interface
line

Precautions

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

2.2.5 *spanning-tree*

Configure protocol parameters for spanning-tree protocol. However, if there is no interface to run spanning tree, there is no need to configure these parameters.

Input Format

Setting information

```
[set] spanning-tree [-priority <Priority>]  [-hello_time <Second>]
[-max_age_time <Second>]  [-forward_delay_time <Second>]
```

Modifying information

```
[set] spanning-tree [-priority <Priority>]  [-hello_time <Second>]
[-max_age_time <Second>]  [-forward_delay_time <Second>]
```

Displaying information

```
show spanning-tree
```

Deleting information

```
delete spanning-tree
```

Parameters

`-priority <Priority>`

Description: This parameter configures 16 high bits of bridge ID (64 bits). The 48 low bits of bridge ID are for the MAC address of the RM Ethernet connecting port. The bridge ID is used to identify root bridge in the spanning-tree algorithm. The smaller the priority value, the higher the priority, and the bridge set with the smallest value is the root bridge.

Default: `32768`

Range of value: `0-65535`

`-hello_time <Second>`

Description: Configures transmission interval, in seconds, of BPDU transmitted by bridge.

Default: `2` (seconds)

Range of value: `1-10`

`-max_age_time <Second>`

Description: Specifies the maximum time, in seconds, to keep the bridge protocol information received. The following conditions must be satisfied: `max_age_time >= (hello_time + 1 ) X 2`

Default: `18` (seconds)

range of value: `6-40`

`-forward_delay_time <Second>`

Description: Specifies time, in seconds, needed for transition of bridge interface states. The following conditions must be satisfied: `(forward_delay_time - 1) X 2 >= max_age_time`

Downloaded from www.Manualslib.com manuals search engine

Default: 10 (seconds)

Range of value: 4-30

Examples

1. Setting parameters

   To set priority for spanning tree to 32768, hello time to 2 seconds, maximum aging time to 20 seconds, and forward delay time to 15:

```
(config)# spanning-tree -priority 32768 -hello_time 2 -max_age_time 20
-forward_delay_time 15
(config)#
```

2. Changing parameters

   To change the priority to 30000, and hello time to 5 seconds:

```
(config)# spanning-tree -priority 30000 -hello_time 5
(config)#
```

3. Displaying setting information

```
(config)# show spanning-tree
  spanning-tree {
      priority 30000 ;
      hello_time 5 ;
      max_age_time 20 ;
      forward_delay_time 15 ;
  } ;
(config)#
```

4. Deleting parameters

   To delete the priority:

```
(config)# show spanning-tree
  spanning-tree {
      priority 30000 ;
      hello_time 5 ;
      max_age_time 20 ;
      forward_delay_time 15 ;
  } ;
(config)#  delete spanning-tree -priority
(config)# show spanning-tree
  spanning-tree {
      hello_time 5 ;
      max_age_time 20 ;
      forward_delay_time 15 ;
  } ;
```

Related Commands

bridge

Downloaded from www.Manualslib.com manuals search engine

Precausion

If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

This page left intentionally blank

Downloaded from www.Manualslib.com manuals search engine

Chapter 3
SNMP Information

3.1 SNMP Objects

The SNMP information objects apply to either SNMP or RMON as shown in Table 3-1 below.

Table 3-1 Application of SNMP Information Objects

Category	Purpose	Object	Subsection
SNMP	To register SNMP Manager	snmp	3.1.1
RMON	To set RMON Ethernet history-group control information	history-control	3.1.2
	To set RMON Ethernet alarm-group information	alarm	3.1.3
	To set RMON Ethernet event-group information	event	3.1.4

Note: These objects must be used in conjunction with the configuration subcommand.

3.1.1 *snmp*

Function

Object for creation, modification, deletion, and display of SNMP Managers. Up to 20 SNMP Managers can be registered per router. For the supported MIB and support trap lists, see the GR2000 Operations Guide.

Input Format

To create or modify an SNMP Manager:

```
[set] snmp <Community Name> <{ SNMP manager IP Address| SNMP manager IPv6
Address }> [{ -read | -read_write }]
[{ -none | -trap | -ex_trap [ -level <Level> ] | -selection_trap }]
[{ -limited_coldstart_trap | -unlimited_coldstart_trap }]
[-link_trap_mode{ -interface | -protocol }]
[-link_trap_bind_info {private | standard}]
[ -trap_version { 1 | 2 }]
[ -bgp_trap ] [ -rmon_trap ] [ -dsx1_trap ] [ -dsx3_trap ] [ -vrrp_trap ]
[ -system_msg_trap [ -level <Level> ] ] [ -standby_system_trap ]
[ -temperature_trap ] [ -atm_pvc_trap ]
```


Downloaded from www.Manualslib.com manuals search engine

To delete an SNMP Manager:

```
delete snmp <Community Name> <SNMP Manager IP Address>
```

To display registered SNMP Managers:

```
show snmp
```

Parameters

`<Community Name>`

Description: Specifies the SNMP Manager community name.

Default: Undefined (but cannot be omitted).

Range of value: Same as `router -name <Router Name>`. See Table 2-1, in *GR2000 Configuration Commands, (universal CLI) Vol. 1*.

`{<SNMP manager IP Address> | <SNMP manager IPv6 Address>}`

Description: Specifies the SNMP Manager IP address.

Default: Undefined (but cannot be omitted)

Range of value: Specify IP address (dot notation) in <SNMP manager IP address> or specify IPv6 address (colon notation) in <SNMP manager IPv6 address>.

`{-read | -read_write}`

Description: Sets the MIB operation mode for the specified SNMP Manager. When -read is specified, Get Request and GetNext Request are permitted. When -read_write is specified, Get Request, GetNext Request, and Set Request are permitted.

Default: read

Range of value: read or read-write

`{-none | -trap | -ex_trap | selection_trap}`

Description: Sets the trap transmission mode for the specified SNMP Manager. When *none* is specified, no trap is performed. When trap is specified, the standard trap is enabled. When ex_trap is specified, both the standard trap and the private trap are enabled. The individually specified trap is issued when selection_trap is specified.

Default: none

Range of value: Select none, trap, ex-trap or selection_trap

`-level <Level>`

Description: Sets the transmission level of the system messages for the private trap. This parameter is valid only when the trap transmission mode is ex_trap or system_msg_trap. Table 3-2 displays the list of system messages to transmitted by the private trap depending on the level specified by this parameter.

Default: 9

Range of value: 1 to 9 (decimal) is specified in <Level>.

Downloaded from www.Manualslib.com manuals search engine

Caution: When 1 to 3 is specified in <Level>, the operation is the same as when 3 is specified.

Table 3-2 Trap System Message Levels

Level	Meaning
9	Fatal failure.
8	Serious failure or greater.
7	RM failure or greater.
6	NIF failure or greater.
5	Standby system failure or greater.
4	Network system failure or greater.
1-3	Warning level or greater.

`{-limited_coldstart_trap | -unlimited_coldstart_trap}`

This parameter limits the moment at which coldstart trap is issued. The moment at which coldstart trap is issued during setting of this parameter is outlined in the table below.

Parameter	Moment at Which *coldstart trap* is Issued
limited_coldstart_trap	• When the router starts (the router power is turned on or active RM restarts). • When active RM is switched to standby RM. • When the current configuration definition information is changed using a *config copy* command. • When the configuration information (*config ip* command) of IP is added and deleted. • When the time is changed using a *date* command
unlimited_coldstart_trap	• When the router starts (the router power is turned on or active RM restarts). • When active RM is switched to standby RM.

Default: limited_coldstart_trap

Range of value: limited_coldstart_trap or unlimited_coldstart_trap is specified.

`-link_trap_mode{interface | protocol}`

This parameter specifies the moment at which link up/down trap is issued. The moment at which link up/down trap is issued during setting of this parameter is outlined in the table below.

Parameter	Moment at Which link up/down trap is Issued
Interface	• Traps are sent prompted by up/down in the physical interface.
Protocol	• Traps are sent prompted by link connection and disconnection at the protocol level.

Default: protocol

Range of value: interface or protocol is specified.

Downloaded from www.Manualslib.com manuals search engine

-link_traop_bind_info{private | standard}

Setting is made for the purpose of selecting MIBs appended at the time when link up/down traps are issued.

MIBs appended at the time of link up/down trap issuance by the setting of this parameter are indicated in the table below.

Parameter	Moment at Which link up/down trap is Issued
Interface	• (SNMPv1/SNMPv2 trap common) ifIndex, ifDescr, ifType
Protocol	• (In case of SNMPv1 trap) ifIndex, • (In case of SNMPv2 trap) ifIndex, ifAdminStatus, ifOperStatus

Default: standard

Range of value: private or standard is specified.

-trap version { 1 | 2 }

Description: Sets the trap transmission version to the manager of the specified IP address that belongs to the specified community name. The trap of an SNMPv1 version is issued when "1" is specified. The trap of an SNMPv2 version is issued when "2" is specified.

Default: 1

Range of value: Specifies "1" or "2".

-bgp_trap

This parameter transmits the trap in case that a BGP link is established and disconnected when the Trap transmission mode is selection_trap.

-rmon_trap

This parameter transmits the trap in case the upward threshold value of an rmon alarm is exceeded and the downward threshold value is not exceeded when the Trap transmission mode is selection_trap.

-dsx1_trap

This parameter transmits the trap in case the state of E1 and T1 interfaces change when the trap transmission mode is selection_trap.

-dsx3_trap

This parameter transmits the trap in case the state of T3, E3, CE3, and CT3 interfaces change when the trap transmission mode is selection_trap.

-vrrp_trap

This parameter transmits the trap in case the state of vrrp changes when the Trap transmission mode is selection_trap.

-system_msg_trap

This parameter transmits the trap in case a system message is output when the Trap transmission mode is selection_trap.

-standby_system_trap

This parameter transmits the trap in case standby RM is put into the UP/DOWN state when the Trap transmission mode is selection_trap.

Downloaded from www.Manualslib.com manuals search engine

-temperature_trap

This parameter transmits the trap in case the temperature state changes when the Trap transmission mode is selection_trap.

-atm_pvc_trap

This parameter transmits the trap in case a PVC failure is notified when the trap transmission mode is selection_trap.

Examples

1. Create the following SNMP Manager entries, and show the resulting SNMP Manager information:
   - SNMP Manager with IP address 10.1.1.1, community name “public,” and read-only MIB access
   - SNMP Manager with IP address 20.1.1.1, community name “public,” and read/write MIB access
   - SNMP managers that permit MIB access in the read/write mode in community name "event-monitor" and IP address 30.1.1.1 and send "bgpEstablished," "bgpBackwardTransition," "risingAlarm" and "fallingAlarm" traps
   - SNMP managers that permit MIB access in the read mode in community name "private" and IP address 40.1.1.1, limit opportunities for the issuance of the cold start trap and send version 2 of the standard trap
   - SNMP managers that permit MIB access in the read/write mode in community name "public-v6" and IP address 3ffe::|.

```
(config)# snmp "public" 10.1.1.1 -read
(config)# snmp "public" 20.1.1.1 -read_write
(config)# snmp "event-monitor" 30.1.1.1 -read_write -selection_trap
-bgp_trap -rmon_trap
(config)# snmp "private" 40.1.1.1 -read -trap -limited_coldstart_trap
-trap_version 2
(config)# snmp "public-v6" 3ffe::| -read_write
(config)# show snmp
snmp {
        "public" {
                  20.1.1.1 read_write;
                  10.1.1.1 read;
         };
        "event-monitor" {
                30.1.1.1 read_write selection_trap {
                        bgp_trap;
                        rmon_trap;
                };
        };
        "private" {
                 40.1.1.1 read trap limited_coldstart_trap trap_version 2;
        };
        "public-v6" {
                  3ffe::| read_write;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Modify registered SNMP Managers in the following manner, and show the resulting SNMP Manager information:
   - Setting of SNMP Manager with IP address 10.1.1.1 and community name “public”: Enable private trap in system message level 7 (RM failure or greater).
   - Setting of SNMP Manager with IP address 30.1.1.1 and community name “event-monitor”: Change MIB access to read only

```
(config)# snmp "public" 10.1.1.1 -ex_trap -level 7
(config)# snmp "event-monitor" 30.1.1.1 -read
(config)# show snmp
snmp {
        "public" {
                  20.1.1.1 read_write;
                  10.1.1.1 read ex_trap level 7;
        };
        "event-monitor" {
                30.1.1.1 read selection_trap {
                        bgp_trap;
                        rmon_trap;
                };
        };
        "private" {
                 40.1.1.1 read trap limited_coldstart_trap trap_version 2;
        };
        "public-v6" {
                  3ffe::| read_write;
        };
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Display register status of SNMP Manager:

```
(config)# show snmp
snmp {
        "public" {
                  20.1.1.1 read_write;
                  10.1.1.1 read ex_trap level 7;
        };
        "event-monitor" {
                30.1.1.1 read selection_trap {
                        bgp_trap;
                        rmon_trap;
                };
        };
        "private" {
                 40.1.1.1 read trap limited_coldstart_trap trap_version
2;
        };
        "public-v6" {
                  3ffe::| read_write;
        };
};
(config)#
```

Delete part of SNMP Managers and show the resulting SNMP Manager information:

```
(config)# delete snmp "public" 10.1.1.1
(config)# delete snmp "event-monitor" 30.1.1.1
(config)# show snmp
snmp {
        "public" {
                  20.1.1.1 read_write;
        };
        "private" {
                40.1.1.1 read trap limited_coldstart_trap trap_version 2;
        };
        "public-v6" {
                  3ffe::| read_write;
        };
};
(config)#
```

Related Configuration Object

None

Related Information

For the support MIB and Trap, refer to the *GR2000 Operations Log and MIB Reference*.

Precautions

Five standard traps (cold start, warm start, link up, link down, and authentication failure) as well as the individually specified trap are issued when selection_trap is specified.

Downloaded from www.Manualslib.com manuals search engine

3.1.2 history-control

Function

Object for creation, modification, deletion, and display of RMON (RFC1757) Ethernet history-group control information. A maximum of 32 history-group control entries can be registered per router.

Input Format

To create an RMON Ethernet history-group control entry:

```
[set] history-control <Index> -interface <Line Name>
[ -buckets_requested <Number> ] [ -interval <Seconds> ]
[ -owner <String> ]
```

To modify an RMON Ethernet history-group control entry:

```
[set] history-control <Index> [ -interface <Line Name> ]
[ -buckets_requested <Number> ] [ -interval <Seconds> ]
[ -owner <String> ]
```

To delete registered RMON Ethernet history-group control entries:

```
delete history-control <Index>
```

To show registered RMON Ethernet history-group control entries:

```
show history-control [ <Index> ]
```

Parameters

`<Index>`

Description: Specifies the RMON Ethernet history-group control index number. This parameter corresponds to historyControlIndex of RFC1757.

Default: Undefined (but cannot be omitted)

Range of value: 1-65535

`-interface <Line Name>`

Description: Specifies the Ethernet line name subject to acquisition of the RMON Ethernet history. This parameter corresponds to historyControlDataSource of RFC1757.

Default: Undefined (but cannot be omitted)

Range of value: Line name defined by the line subcommand

`-buckets_requested <Number>`

Description: Sets the number of RMON Ethernet history-group control entries. This parameter corresponds to historyControlBucketsRequested of RFC1757.

Default: 50

Range of value: 1-65535

Downloaded from www.Manualslib.com manuals search engine

`-interval <Seconds>`

Description: Sets the interval of time in seconds for collecting RMON Ethernet history events. This parameter corresponds to historyControlInterval of RFC1757.

Default: 1800

Range of value: 1-3600

`-owner <String>`

Description: Sets the identification information for the person who created this setting. This parameter corresponds to historyControlOwner of RFC1757.

Default: Blank

Range of value: A string of up to 24 alphanumeric and special characters enclosed in double quotation marks. When the string contains only alphanumeric characters and no special characters except period, you can omit double quotation marks. See Table 2-1, in *GR2000 Configuration Commands, (universal CLI) Vol. 1*. for allowable characters.

Example

Create RMON Ethernet history-group control entries and show the resulting history-group control entries in the following order:

1. Using the snmp object with the set subcommand omitted, create an SNMP Manager entry with the following properties:
   - Community name: public
   - SNMP Manager IP address: 30.1.1.1
   - MIB access mode: read/write
2. Using the line object with the set subcommand omitted, set the Ethernet line information with the following properties. (The IP address must be predefined.)
   - Line name: kyoto
   - NIF/line number: 0/0
3. Using the line object with the set subcommand omitted, set the Gigabit Ethernet line information with the following properties. (The IP address must be predefined.)
   - Line name: osaka
   - NIF/line number: 4/0
4. Using the history-control object with the set subcommand omitted, create an RMON Ethernet history-group control entry for the above-mentioned Ethernet line with the following properties:
   - RMON Ethernet history-group control index number: 33
   - Interface name: kyoto
   - Number of history-group entries: 10
   - Owner: “net-mgr ken”
5. Using the history-control object with the set subcommand omitted, set the RMON Ethernet history-group control entry for the above-mentioned Gigabit Ethernet line with the following properties:

Downloaded from www.Manualslib.com manuals search engine

- RMON Ethernet history-group control index number: 45
- Interface name: osaka
- Interval: 2000 seconds
- Owner: “net-mgr ken”

6. Show the resulting history-group control entries.

```
(config)# snmp public 30.1.1.1 -read_write
(config)# line kyoto ethernet 0/0
(config)# line osaka gigabit_ethernet 4/0
(config)# history-control 33 -interface kyoto -buckets_requested 10
-owner "net-mgr ken"
(config)# history-control 45 -interface osaka -interval 2000 -owner
"net-mgr ken"
(config)# show history-control
history_control 33 {
    interface kyoto;
    buckets_requested 10;
    owner "net-mgr ken" ;
};
history_control 45 {
    interface osaka;
    interval 2000;
    owner "net-mgr ken" ;
};
(config)#
```

7. Modify the number of history-group control entries for RMON Ethernet history-group control index number 33 from 10 entries to 20 entries, and show the resulting history-group control entries:

```
(config)# history-control 33 -buckets_requested 20
(config)# show history-control
    history_control 33 {
        interface kyoto;
        buckets_requested 20;
        owner "net-mgr ken" ;
    };
    history_control 45 {
        interface osaka;
        buckets_requested 30;
        interval 2000;
        owner "net-mgr ken" ;
    };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

1. Show the registration status of RMON Ethernet history-group control entry.

```
(config)# show history-control
    history_control 33 {
        interface kyoto;
        buckets_requested 20;
        owner "net-mgr ken" ;
    };
    history_control 45 {
        interface osaka;
        buckets_requested 30;
        interval 2000;
        owner "net-mgr ken" ;
    };
(config)#
```

2. Delete registered RMON Ethernet history-group control entry with index number 33, and show the resulting history-group control entries:

```
(config)# delete history-control 33
(config)# show history-control
    history_control 45 {
        interface osaka;
        buckets_requested 30;
        interval 2000;
        owner "net-mgr ken" ;
    };
(config)#
```

Related Configuration Object

line

snmp

Related Information

The MIB value of an RMON Ethernet history group can be referenced using an SNMP manager or this router's snmp command. For the snmp command, refer to the *GR2000 Operations Commands, Vol. 1*.

Precautions

1. In order to access the history-group control information from an SNMP Manager, you must register the SNMP Manager.
2. When RMON historyControlTable is sent from an SNMP Manager, the change is not reflected in the router's configuration.
3. Prior to deleting any line information, delete the relevant history-group control entry (or entries) first.
4. When IP information is deleted or NIF is closed, you cannot monitor histories on those interfaces. The response will show "invalid(4)" for the value of "History Control Status." Such response may take longer than expected if the period value is set to a high value (estimated response time is half the period value).
5. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

3.1.3 *alarm*

Function

Object for creation, modification, deletion, and display of RMON (RFC1757) Ethernet alarm-group information. A maximum of 128 alarm-group entries can be registered per router. The RMON Ethernet alarm-group MIB contents can be referenced by the device management command snmp. For this snmp command, see the GR2000 Operations Guide.

Input Format

To create an RMON Ethernet alarm-group entry:

```
[set] alarm <Index> -variable <Object ID> -interval <Seconds>
-sample_type { delta | absolute }
[ -startup_alarm { rising_falling | rising | falling } ]
-rising_threshold <Value> -rising_event_index <Number>
-falling_threshold <Value> -falling_event_index <Number>
[ -owner <String> ]
```

To modify an RMON Ethernet alarm-group entry:

```
[set] alarm <Index> [ -variable <Object ID> ] [ -interval <Seconds> ]
[ -sample_type { delta | absolute } ]
[ -startup_alarm { rising_falling | rising | falling } ]
[ -rising_threshold <Value> ] [ -rising_event_index <Number> ]
[ -falling_threshold <Value> ] [ -falling_event_index <Number> ]
[ -owner <String> ]
```

To delete registered RMON Ethernet alarm-group entries:

```
delete alarm <Index>
```

To show registered RMON Ethernet alarm-group entries:

```
show alarm [ <Index> ]
```

Parameters

`<Index>`

Description: Specifies the RMON Ethernet alarm-group index number. This parameter corresponds to alarmIndex of RFC1757.

Default: Undefined (but cannot be omitted)

Range of value: 1-65535

`-variable <Object ID>`

Description: Sets the object ID of the MIB that checks out the alarm threshold. This parameter corresponds to alarmVariable of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: Object ID of counter or gauge type in up to 63 alphanumeric and special characters in dot format enclosed by double quotation marks. When the string contains only alphanumeric characters and no special characters except period, you can omit double quotation marks.

Downloaded from www.Manualslib.com manuals search engine

`-interval <Seconds>`

Description: Sets the interval of time in seconds for checking out the alarm threshold. This parameter corresponds to alarmInterval of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: 1-4294967295

`-sample_type { delta | absolute }`

Description: Sets the method for checking out the alarm threshold. The `delta` option compares the threshold number of packets with the differences between the current samples and the previous samples. The `absolute` option compares the threshold number of packets directly with the current samples. This parameter corresponds to alarmSampleType of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: delta or absolute

`-startup_alarm { rising_falling | rising | falling }`

Description: Sets the alarm threshold for RMON startup alarm. The `rising` option causes an alarm if the first sampling exceeds the rising (upper-limit) threshold number of packets. The `falling` option causes an alarm if the first sampling falls short of the falling (lower-limit) threshold number of packets. The `rising_falling` option causes an alarm if the first sampling exceeds the rising threshold or falls short of the falling threshold. This parameter corresponds to alarmstartUpAlarm of RFC1757.

Default: `rising_falling`.

Range of value: rising, falling or rising-falling

`-rising_threshold <Value>`

Description: Sets the rising threshold number of packets for RMON alarm other than startup. This parameter corresponds to alarmRisingThreshold of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: 1-4294967295

`-rising_event_index <Number>`

Description: Sets the index number for an RMON event-group entry exceeding the rising threshold. Such index number must be equal to the RMON event-group index number defined by the event object. When no ID number has been defined, an alarm is not issued. This parameter corresponds to alarmRisingEventIndex of RFC1757.

Default: Undefined (but cannot be omitted for the first time).

Range of value: 1-65535

Downloaded from www.Manualslib.com manuals search engine

`-falling_threshold <Value>`

Description: Sets the falling threshold number of packets for RMON alarm other than startup. This parameter corresponds to alarmFallingThreshold of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: 1-4294967294

`-falling_event_index <Number>`

Description: Sets the index number for an RMON event-group entry falling short of the falling threshold. Such index number must be equal to the RMON event-group index number defined by the event object. When no ID number has been defined, an alarm is not issued. This parameter corresponds to alarmFallingEventIndex of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: 1-65535

`-owner <String>`

Description: Sets the identification information for the person who created this setting. This parameter corresponds to alarmOwner of RFC1757.

Default: Blank

Range of value: A string of up to 24 alphanumeric and special characters enclosed in double quotation marks. When the string contains only alphanumeric characters and no special characters except period, you can omit double quotation marks. See Table 2-1, in *GR2000 Configuration Commands, (universal CLI) Vol. 1* for allowable characters.

Example

Create RMON Ethernet alarm-group entries and show the resulting alarm-group entries in the following order:

1. Using the snmp object with the set subcommand omitted, create an SNMP Manager entry with the following properties:
   - Community name: public
   - SNMP Manager IP address: 30.1.1.1
   - MIB access mode: read/write
   - Trap option: trap
2. Using the event object with the set subcommand omitted, create an event-group entry with the following properties:
   - RMON Ethernet event-group index number: 3
   - Event type: log_trap
   - Trap community name: public
3. Using the alarm object with the set subcommand omitted, create an RMON Ethernet alarm-group entry with the following properties for the above event-group entry:
   - RMON Ethernet alarm-group index number: 12

Downloaded from www.Manualslib.com manuals search engine

- Object MIB ID: “1.3.6.1.2.1.2.2.1.19.3” (= “ifOutDiscards.3”)
  Note: ifOutDiscards MIB counts discarded packets for which no error is detected.
- Interval: 256111 seconds
- Sample type: delta
- Rising threshold: 400000 packets
- Rising event index number: 3
- Falling threshold: 100 packets
- Falling event index number: 3
- Owner: “net-mgr ken 07/25”

4. Using the alarm object with the set subcommand omitted, create another RMON Ethernet alarm-group entry with the following properties for the same event-group entry:
   - RMON Ethernet alarm-group index number: 20
   - Object MIB ID: “ifOutDiscards.4”
   - Interval: 12800 seconds
   - Sample type: absolute
   - Rising threshold: 30000 packets
   - Rising event index number: 3
   - Falling threshold: 300 packets
   - Falling event index number: 3
   - Owner: “net-mgr ichiro 07/25”

Downloaded from www.Manualslib.com manuals search engine

5. Show the resulting alarm-group entries.

```
(config)# snmp public 30.1.1.1 -read_write trap
(config)# event 3 -type log_trap -community public
(config)# alarm 12  -variable "1.3.6.1.2.1.2.2.1.19.3"  -interval
256111 -sample_type  delta -rising_threshold 400000
-rising_event_index 3 -falling_threshold 100  -falling_event_index 3
-owner "net-mgr ken 07/25"
(config)# alarm 20  -variable "ifOutDiscards.4"  -interval  12800
-sample_type absolute -rising_threshold 30000 -rising_event_index 3
-falling_threshold 300 -falling_event_index 3 -owner "net-mgr ichiro
07/25"
(config)# show alarm
    alarm 12 {
          variable  "1.3.6.1.2.1.2.2.1.19.3" ;
         interval 256111;
         sample_type delta;
         rising_threshold 400000;
         rising_event_index 3;
         falling_threshold 100;
         falling_event_index 3;
        owner "net-mgr ken 07/25";
    };
    alarm 20 {
        variable  "ifOutDiscatds.4" ;
        interval 128000;
        sample_type absolute;
        rising_threshold 30000;
        rising_event_index 3;
        falling_threshold 300;
        falling_event_index 3;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Change the interval setting for RMON Ethernet alarm-group index number 12 to 256 seconds and show the resulting alarm-group entries:

```
(config)# alarm 12 -interval 256
(config)# show alarm
    alarm 12 {
        variable  "1.3.6.1.2.1.2.2.1.19.3" ;
        interval 256;
        sample_type delta;
        rising_threshold 400000;
        rising_event_index 3;
        falling_threshold 100;
        falling_event_index 3;
        owner "net-mgr ken 07/25";
    };
    alarm 20 {
        variable  "ifOutDiscatds.4" ;
        interval 128000;
        sample_type absolute;
        rising_threshold 30000;
        rising_event_index 3;
        falling_threshold 300;
        falling_event_index 3;
       owner "net-mgr ichiro 07/25";
    };
(config)#
```

Show the registration status of RMON alarm-group control entry:

```
(config)# show alarm
    alarm 12 {
        variable  "1.3.6.1.2.1.2.2.1.19.3" ;
        interval 256;
        sample_type delta;
        rising_threshold 400000;
        rising_event_index 3;
        falling_threshold 100;
        falling_event_index 3;
        owner "net-mgr ken 07/25";
    };
    alarm 20 {
        variable  "ifOutDiscatds.4" ;
        interval 128000;
        sample_type absolute;
        rising_threshold 30000;
        rising_event_index 3;
        falling_threshold 300;
        falling_event_index 3;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Delete registered RMON Ethernet alarm entry with index number 12 and show the resulting alarm-group entries:

```
(config)# delete alarm 12
(config)# show alarm
    alarm 20 {
        variable  "ifOutDiscatds.4" ;
        interval 128000;
        sample_type absolute;
        rising_threshold 30000;
        rising_event_index 3;
        falling_threshold 300;
        falling_event_index 3;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```

Related Configuration Objects

`event`

`snmp`

Related Information

The MIB value of an RMON Ethernet history group can be referenced using an SNMP manager or this router's snmp command. For the snmp command, refer to the *GR2000 Operations Commands, Vol. 1*.

Precautions

1. In order to access the Ethernet alarm-group information from an SNMP Manager, you must register the SNMP Manager.
2. Make sure that the `rising_event_index` and `falling_event_index` settings are equal to those defined by the event object. If any discrepancy exists, the event is not executed in response to an alarm.
3. When RMON alarmTable is sent from an SNMP Manager, the change is not reflected in the router's configuration.
4. When a high number of items are specified by the `alarm` object or the `interval` setting is specified no more than 60 seconds, certain alarms may fail to obtain the target MIB, resulting in no alarm activation and "invalid(4)" response from the alarmStatus MIB. Should such incident occur, delete unnecessary `alarm` object setting items or increase the `interval` setting to longer than 60 seconds.
5. A longer `interval` setting requires more time for the historyControlStatus change from valid(1) to invalid(4). Estimated transition time is half the `interval` setting.
6. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

3.1.4 *event*

Function

Object for creation, modification, deletion, and display of RMON (RFC1757) Ethernet event-group information. A maximum of 16 event-group entries can be registered per router. The RMON Ethernet event-group MIB contents can be referenced by the device management command snmp. For this snmp command, see the *GR2000 Operations Commands, Vol. 1*.

Input Format

To create an RMON Ethernet event-group entry:

```
[set] event <Index> -type { none | log | trap | log_trap }
      [ -community <Trap Community Name> ] [ -description <String> ]
      [ -owner <String> ]
```

To modify an RMON Ethernet event-group entry:

```
[set] event <Index> [ -type { none | log | trap | log_trap } ]
      [ -community <Trap Community Name> ] [ -description <String> ]
      [ -owner <String> ]
```

To delete registered RMON Ethernet event-group entries:

```
delete event <Index>
```

To show registered RMON Ethernet event-group entries:

```
show event [ <Index> ]
```

Parameters

`<Index>`

Description: Specifies the RMON Ethernet event-group index number. This parameter corresponds to eventIndex of RFC1757.

Default: Undefined (but cannot be omitted)

Range of value: 1-65535

`-type { none | log | trap | log_trap }`

Description: Sets the method for alarming the specified event. The none option causes no alarm. The log option records every alarmed event. The trap option causes transmission of SNMP trap to the specified community. The log_trap option records every alarmed event and causes transmission of SNMP trap to the specified community. This parameter corresponds to eventType of RFC1757.

Default: Undefined (but cannot be omitted for the first time)

Range of value: none, log, trap or log-trap

`-community <Trap Community Name>`

Description: Sets the community to which an SNMP trap is transmitted when the trap or log_trap option is specified for the -type parameter. The -community parameter corresponds to eventCommunity of RFC1757.

Downloaded from www.Manualslib.com manuals search engine

Default: Undefined

Range of value: A string of up to 60 alphanumeric and special characters enclosed in double quotation marks. When the string contains only alphanumeric characters and no special characters except period, you can omit double quotation marks. See Table 2-1, in *GR2000 Configuration Commands, (universal CLI) Vol. 1* for allowable characters.

`-description <String>`

Description: Serves as a comment field where you can describe the event-group contents using a character string. This parameter corresponds to eventDescription of RFC1757.

Default: Brank

Range of value: A string of up to 79 alphanumeric and special characters enclosed in double quotation marks. When the string contains only alphanumeric characters and no special characters except period, you can omit double quotation marks. See Table 2-1, in *GR2000 Configuration Commands, (universal CLI) Vol. 1* for allowable characters.

`-owner <String>`

Description: Sets the identification information for the person who created this setting. This parameter corresponds to eventOwner of RFC1757.

Default: Blank

Range of value: A string of up to 24 alphanumeric and special characters enclosed in double quotation marks. When the string contains only alphanumeric characters and no special characters except period, you can omit double quotation marks. See Table 2-1, in *GR2000 Configuration Commands, (universal CLI) Vol. 1* for allowable characters.

Example

Create RMON Ethernet event-group entries and show the resulting event-group entries in the following order:

1. Using the snmp object with the set subcommand omitted, create an SNMP Manager entry with the following properties:
   - Community name: rmon-mgr
   - SNMP Manager IP address: 30.1.1.1
   - MIB access mode: read/write
   - Trap option: trap
2. Using the event object with the set subcommand omitted, create an event-group entry with the following properties:
   - RMON Ethernet event-group index number: 3
   - Event type: trap
   - Trap community name: rmon-mgr
3. Using the event object with the set subcommand omitted, create another event-group entry with the following properties:
   - RMON Ethernet event-group index number: 3

Downloaded from www.Manualslib.com manuals search engine

- Event type: log
- Trap community name: “net-mgr ichiro 07/25”

4. Using the alarm object with the set subcommand omitted, create an RMON Ethernet alarm-group entry with the following properties for the above event-group entries:
   - RMON Ethernet alarm-group index number: 12
   - Object MIB ID: “ifOutDiscards.3”
     Note: ifOutDiscards MIB counts discarded packets for which no error is detected.
   - Interval: 256111 seconds
   - Sample type: delta
   - Rising threshold: 400000 packets
   - Rising event-group index number: 3
   - Falling threshold: 100 packets
   - Falling event-group index number: 5
5. Show the resulting event-group entries.

```
(config)# snmp "rmon-mgr" 30.1.1.1 -read_write trap
(config)# event 3 -type trap -community "rmon-mgr"
(config)# event 5 -type log -owner "net-mgr ichiro 07/25"
(config)# alarm 12  -variable "ifOutDiscards.3"  -interval  256111
-sample_type  delta -rising_threshold 400000 -rising_event_index 3
-falling_threshold 100  -falling_event_index 5
(config)# show event
    event 3 {
        type trap;
        community "rmon-mgr";
    };
    event 5 {
        type log;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```

Add description and owner to the registered event-group index number 3, and show the resulting event-group entries:

```
(config)# event 3 -description "if inInError > 200 then trap" -owner
"monitor"
(config)# show event
    event 3 {
        type trap;
        community "rmon-mgr";
        description "if inInError > 200 then trap";
        owner "monitor";
    };
    event 5 {
        type log;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Show the registration status of RMON event-group entry:

```
(config)# show event
    event 3 {
        type trap;
        community "rmon-mgr";
        description "if inInError > 200 then trap";
        owner "monitor";
    };
    event 5 {
        type log;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```

Delete registered RMON Ethernet event-group entry with the event-group index number 3, and show the resulting event-group entries:

```
(config)# delete event 3
(config)# show event
    event 5 {
        type log;
        owner "net-mgr ichiro 07/25";
    };
(config)#
```

Related Configuration Objects

alarm

snmp

Related Information

The MIB value of an RMON Ethernet history group can be referenced using an SNMP manager or this router's snmp command. For the snmp command, refer to *GR2000 Operations Commands, Vol. 1*.

Precautions

1. In order to access the Ethernet event-group information from an SNMP Manager or issue a trap to an SNMP Manager, you must register the SNMP Manager. For the latter purpose, specify -trap or -ex_trap option in the registration action.
2. Make sure that the rising_event_index and falling_event_index settings are equal to those defined by the alarm object. If any discrepancy exists, the event is not executed in response to an alarm.
3. Make sure that the community setting is equal to the one defined by the snmp object. If any discrepancy exists, no trap is transmitted in the specified event.
4. When RMON eventTable is sent from an SNMP Manager, the change is not reflected in the router's configuration.
5. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

Chapter 4
Operation Management Information

4.1 Host Name Information

Note: This object must be used in conjunction with the configuration subcommand.

4.1.1 *hosts*

The host name can be specified for identifying each device on the network, e.g., when configuring log information or NTP information.

Function

Specifies host name information. Up to 20 host names can be registered.

Input format

To create a host name entry:

```
[set] hosts { <IP address> | <IPv6 Address> } <host name>
```

To delete a host name entry:

```
delete hosts { <IP address> | <IPv6 Address> }
```

To show a host name entry:

```
show hosts
```

Parameter

`{ <IP Address> | <IPv6 Address> }`

Description: Specifies the target IPv4 address in dot notation and IPv6 address in colon nation.

`<host name>`

Description: Specifies the host name to be added to the target IPv4 or IPv6 address.

Downloaded from www.Manualslib.com manuals search engine

Example

Create a host name entry and show the result (IPv4):

```
(config)#  hosts 10.1.1.1 loghost
(config)#  show hosts
hosts {
    10.1.1.1 loghost;
};
(config)#
```

Create a host name entry and show the result (IPv6):

```
(config)# hosts 3ffe:501:811:ff01::1 testhost
(config)# show hosts
hosts {
    10.1.1.1 loghost;
    3ffe:501:811:ff01::1 testhost;
};
(config)#
```

Delete a host name entry and show the result (IPv4):

```
(config)# show hosts
hosts {
    10.1.1.1 loghost;
    3ffe:501:811:ff01::1 testhost;
};
(config)# delete hosts 10.1.1.1
Are you sure ?(y/n)y
(config)# show hosts
hosts {
    3ffe:501:811:ff01::1 testhost ;
(config)#
```

Delete a host name entry and show the result (IPv6):

```
(config)# show hosts
hosts {
     3ffe:501:811:ff01::1 testhost;
};
(config)# delete hosts 3ffe:501:811:ff01::1
Are you sure ?(y/n)y
(config)# show hosts
hosts;
(config)#
```

Displaying the configuration information:
To show the host name information:

```
(config)# show hosts
hosts {
    10.1.1.1 loghost;
    3ffe:501:811:ff01::1 testhost;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Precautions

- Multiple host names must not be defined to the same IP or IPv6 address.
- "localhost" must not be defined as the host name.
- "127.*.*.*" must not be defined as the IPv4 address.
- The class D or class E address must not be defined as an IPv4 address.
- Global address and site local address may be specified as the IPv6 addresses.
- If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
- Host names are not distinguished with capital letters and small letters.
- Do not set multiple IP and IPv6 addresses in the same host name.

4.1.2 *dns-resolver*

Function

Sets DNS resolver information.

Input Format

To set own host name:

```
[set] dns-resolver -hostname <host name>
```

To set domain name:

```
[set] dns-resolver -domain <Local domain name>
```

To set name server:

```
[set] dns-resolver nameserver <IP Address>
```

To set DNS resolver function:

```
[set] dns-resolver {yes | no}
```

To set the relay function's effectiveness and ineffectiveness:

```
[set] dns-resolver-relay {yes | no}
```

To delete DNS resolver information:

```
delete dns-resolver
```

To delete name server:

```
delete dns-resolver nameserver <IP Address>
```

To delete the relay function setting information:

```
delete dns-resolver --relay
```

To delete own host name:

```
delete dns-resolver --hostname
```


Downloaded from www.Manualslib.com manuals search engine

To delete domain name:

```
delete dns-resolver --domain
```

To show information:

```
show dns-resolver
```

Parameter

```
<host name>
```

Description: Specifies host name of this router.

```
<local domain name>
```

Description: Specifies domain name of this router.

```
<IP Address>
```

Description: Specifies IP address of name server in dot.

Example

1. Set of DNS resolver
   Set DNS resolver with own host name as router-1.mydomain.com, domain name as mydomain.com, and nameserver as 192.168.0.1:

```
(config)#  dns-resover -hostname router-1.mydomain.com
(config)#  dns-resolver nameserver 192.168.0.1
(config)#  dns-resolver -domain mydomain.com
(config)#  dns-resolver yes
(config)#  show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
};
(config)#
```

2. Invalidity of DNS resolver
   Set DNS resolver to invalid with its definition being left:

```
(config)#  show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
};
(config)#  dns-resolver no
(config)#  show dns-resolver
dns_resolver no {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

3. Showing of setting information
   Show DNS resolver information:

```
(config)#  show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
};
(config)#
```

4. Deletion of setting information
   Delete DNS resolver information:

```
(config)#  show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
};
(config)#  delete dns-resolver
are you sure? (y/n) y
(config)#
```

5. Effectuation of the DNS relay
   Effectuates the DNS function.

```
(config)# dns-resolver relay yes
(config)# show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
  relay yes
};
(config)#
```

6. Invalidity of DNS relay
   Set DNS relay to invalid

```
(config)# dns-resolver relay no
(config)# show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
  relay no
};
(config)#
```

7. Invalidity of DNS relay (Deletion of information)
   Set DNS relay to invalid and delete the information

```
(config)# delete dns-resolver -relay
(config)# show dns-resolver
dns_resolver yes {
  hostname router-1.mydomain.com;
  nameserver 192.168.0.1;
  domain mydomain.com;
};
(config)#
```

Related Commands

None

Downloaded from www.Manualslib.com manuals search engine

Precautions

- Only one host name can be defined to this router.
- Only one domain name can be defined to this router.
- Up to 3 name servers can be specified.
- Name server and domain name cannot be defined unless host name of this router is specified.
- Domain name cannot be specified unless name server is specified.
- localhost cannot be defined as host name.
- Set the DNS server's IP address (dns resolver nameserver) correctly. If the DNS server's IP address is not set correctly, it will take a long time to detect the interruption in communication with the DNS when the host name is referred, disrupting operation. (The time required to display a log in prompt increases when remotely connected to this device via telnet).

The nslookup command can be used as a method to confirm the DNS server. If the "nslookup-retry=1" command, which is the IP address of the DNS server for the host name to be referred, is executed, the host information specified as follows will be displayed when the DNS server's IP address is correct.

Server: Host name in the DNS server.

Address: IP address in the DNS server.

Name: The designated host name.

Address: Designated host's IP address.

If the IP address of the DNS server is not correct, the following indication will be displayed.

*** Can't find server name for address, the IP address of the DNS server: Timed out.

- 127.*.*.* cannot be specified as IP address.
- Class D and class E addresses cannot be specified as IP address.
- Up to 255 characters can be used for host name and domain name. Up to 80 characters can be used for browser.
- It is not possible to refer to the AAA query information by using the IPv6. The AAA query information is referred by using the IPv4.
- If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
- To effectuate the relay function, it is also necessary to effectuate the DNS resolver function.

Downloaded from www.Manualslib.com manuals search engine

4.2 Log Information

Caution: Regarding log Information, this object must be used in conjunction with the configuration subcommand. LOG information can be sent to other devices on the network by the following methods:
1. Sends to the device with syslog function (UNIX workstation, etc.) by using syslog interface. This function enables centralized control of log when controls many devices.
2. Sends by e-mail. This function enables centralized control of log when controls many devices.

4.2.1 *logger-syslog*

Function

Object for creation, deletion, and display of the logger setup, i.e., configuration information necessary for log information output on the syslog interface. Up to 20 of such entries can be registered.

Input format

To create a logger setup entry:

```
[set] logger syslog <host name> <level> <event level>
```

To delete a logger setup entry:

```
delete logger syslog <host name> <level> <event level>
```

To show a logger setup entry:

```
show logger
```

Parameter

`<host name>`

Description: Specifies the logout destination host name.

`<facility>`

Description: This parameter specifies the facility of syslog.
This parameter specifies one of local0, local1, local2, local3, local4, local5, local6, and local7. The initial value when this parameter is omitted is local0.

`<level>`

Description: Specifies the logout level on the syslog interface. Only one among emerg, alert, crit, err, warning, notice, info, and debug can be selected.

`<event level>`

Description: Specifies the event level for the logout. Only one among key, rsp, rtm, err, evt, mrp, mpl, ip6 and mr6 can be selected.

Downloaded from www.Manualslib.com manuals search engine

Example

1. Setting of log syslog information
   The log of event level evt is set so that it is output to host name loghost as syslog of a notice level.

```
(config)#  logger syslog loghost notice evt
(config)#  show logger
logger {
    syslog loghost notice evt;
};
(config)#
```

2. Deletion of log syslog information
   The setting for outputting the log of event level evt to host name loghost as syslog of a notice level is deleted.

```
(config)#  delete logger syslog loghost notice evt
Are you sure ?(y/n)y
(config)#  show logger
logger;
(config)#
```

3. Displaying the configuration information
   To show the syslog information.

```
(config)# show logger
logger;
    syslog loghost notice evt;
};
(config)#
```

Related Configuration Object

hosts

Precautions

- The destination host name must be predefined with the host object.
- In order to use the syslog setup function, the syslog daemon must be running on the destination host and such destination host must be so configured that it can receive the syslog information sent from this router.
- Do not define the same <event level> more than once in the same outbound destination host.
- When IP address is defined to device itself by router-local_address, the IP address is used as the source address of syslog information.
- This function is capable of only outputting IPv4. Therefore, if the host name with the IPv6 only defined is specified with hosts (host name information) in the output host name, no log information is outputted to the said host.
- If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

4.2.2 *logger-email*

Function

Sets information for output log information by e-mail. Up to 64 entries can be set.

Input Format

To set information:

```
[set] logger email <E-Mail Address> <event level>
```

To set information:

```
[set] logger email <E-Mail Address> <event level>
                   at <HH:MM> [<HH:MM>] [<HH:MM>] [<HH:MM>] [<HH:MM>]
```

To set information:

```
[set] logger email <E-Mail Address> <event level> interval <s> <HH:MM>
```

To delete information:

```
delete logger email <E-Mail Address> <event level>
```

To show information:

```
show logger
```

Parameter

`<E-Mail Address>`

Description: Specifies destination e-mail address. To confirm E-Mail function of the specified mail address, set key of <event level> and input any command. If the mail address is normal, mail is sent whenever a command is entered.

`<event level>`

Description: Specifies event level of output log. Specifies either of key, rsp, rtm, err, evt, mrp, mpl, ip6 or mr6.

`at <HH:MM> [<HH:MM>] [<HH:MM>] [<HH:MM>] [<HH:MM>]`

Description: Specifies the time when e-mail is sent. HH is hour. MM is minute. Up to 5 times can be specified.

`interval <s> <HH:MM>`

Description: Specifies interval and starting time of e-mail sending. s is the interval in second. HH is hour. MM is minute.

Downloaded from www.Manualslib.com manuals search engine

Example

1. Set of log E-Mail information
   Set to send log of event level evt to mail address logger@loghost at 9:00, 13:00, and 17:00:

```
(config)#  logger email logger@loghost evt at 9:00 13:00 17:00
(config)#  show logger
logger {
   email logger@loghost evt at 9:00 13:00 17:00;
};
(config)#
```

2. Deletion of log E-Mail information
   Delete the setting to send log of event level evt to mail address logger@loghost:

```
(config)#  show logger
logger {
   email logger@loghost evt at 9:00 13:00 17:00;
};
(config)#  delete logger email logger@loghost evt
are you sure? (y/n) y
(config)#  show logger
logger;
(config)#
```

3. Showing of setting information
   Show log E-Mail information:

```
(config)#  show logger
logger {
   email logger@loghost evt at 9:00 13:00 17:00;
};
(config)#
```

Related Commands

hosts
logger-smtp
dns_resolver

Precautions

- Destination mail server must be predefined by logger-smtp.
- Host name of this device must be predefined by dns_resolver hostname.
- When parameters *at* and *interval* are not specified, e-mail is sent whenever the corresponding event level log occurs. It is recommended to specify at or interval without the emergency one like err event level.
- Confirm if the specified mail address matches to the one defined to destination mail server. If the sending of e-mail fails, the mail is discarded.
- An IP address is used as the source IP address during communication with a mail server when it is set to the router itself by router-local-address.
- This function can be used only with IR4. Therefore, if the host name with the IPv6 only defined is specified with hosts (host name information) in the SMTP server, the E-mail addressed to the said server is discarded.
- If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

- When using e-mail messages and log e-mail simultaneously, do not set more than 1 entry for log e-mail destination address and 1 entry for SMTP server. If defined with more than 1 entry, e-mail transmissions may be delayed several minutes beyond the set time due to entry count and the load conditions of the SMTP server used for log e-mail and e-mail messages.
- Characters usable in e-mail addresses are limited to lower- and upper-case alphabet, numerals, hyphen (-), dot (.) and "at" sign (@). Note that underscoring cannot be used. In addition, the "@" sign cannot be used at the beginning or end of the address and no more than 1 can be used per address.
- The e-mail address length is limited to a maximum of 255 characters. All characters beyond 255 are ignored if 256 or more characters are set.

4.2.3 *logger-email-from* (Log E-Mail Transmission Source Information)

Function

Sets transmission source for output log information by e-mail. One entries can be set.

Input Format

To set information:

```
[set] logger email-from <E-Mail Address>
```

To delete information:

```
logger --email-from
```

To show information:

```
show logger
```

Parameter

`<E-Mail Address>`

Description: This parameter specifies the mail address of E-Mail transmission source.

Example

1. Setting of E-Mail transmission source information
   The transmission source used during log E-Mail transmission is set to nobody@router-1.mydomain.com.:

```
 (config)# logger email-from nobody@router-1.mydomain.com
(config)# show logger
logger {
      email-from nobody@router-1.mydomain.com;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

2. Deletion of E-Mail transmission source information
   The setting of log E-Mail transmission source is deleted.:

```
(config)# show logger
logger {
      email-from nobody@router-1.mydomain.com;;
};
(config)# logger --email-from
(config)# show logger
logger;
(config)#
```

3. Display of setting information
   The log E-Mail transmission source information is displayed.:

```
(config)# show logger
logger {
      email-from nobody@router-1.mydomain.com;
};
(config)#
```

Related Commands

hosts
logger-smtp
dns_resolver

Precautions

- Only one log E-Mail transmission source information of this router can be set.
- The From: line is router name <nobody> when the log E-Mail transmission source information of this router is not set. The router name in this case is the name specified using a router command.
- Characters usable in e-mail addresses are limited to lower- and upper-case alphabet, numerals, hyphen (-), dot (.) and "at" sign (@). Note that underscoring cannot be used. In addition, the "@" sign cannot be used at the beginning or end of the address and no more than 1 can be used per address.
- The e-mail address length is limited to a maximum of 255 characters. All characters beyond 255 are ignored if 256 or more characters are set.

4.2.4 *logger-smtp*

Function

Sets SMTP server information for output log information by e-mail. Up to 16 entries can be set.

Input Format

To set information:

```
[set] logger smtp {<host name> | <IP Address>} [port <port number>]
```

To delete information:

```
delete logger smtp {<host name> | <IP Address>}
```

To show information:

```
show logger
```


Downloaded from www.Manualslib.com manuals search engine

Parameter

{<host name> | <IP Address>}

Description: Specifies host name or IP address of SMTP server.

[port <port number>]

Description: Specifies port No. of SMTP server. When omitted, standard value (25) is used.

Example

1. Set of SMTP server information
   Set SMTP server to loghost to be used fro log E-Mail sending:

```
(config)#  logger smtp loghost
(config)#  show logger
logger {
   smtp loghost;
};
(config)#
```

2. Set of SMTP server information
   Set SMTP server to be used for log E-Mail sending to port 10025 of loghost:

```
(config)#  logger smtp loghost port 10025
(config)#  show logger
logger {
   smtp loghost port 10025;
};
(config)#
```

3. Deletion of SMTP server information
   Delete the loghost setting of SMTP server:

```
(config)#  show logger
logger {
   smtp loghost;
};
(config)#  delete logger smtp loghost
are you sure? (y/n) y
(config)#  show logger
logger;
(config)#
```

4. Show of setting information
   Show SMTP server information:

```
(config)#  show logger
logger {
   smtp loghost;
};
(config)#
```

Related Command

hosts
logger-email
dns_resolver

Downloaded from www.Manualslib.com manuals search engine

Precaution

1. Confirm if the specified SMTP server information (host name or IP address, port No.) matches to the one defined to destination SMTP server. If the connection with SMTP server at the sending of e-mail fails, the mail is discarded.
2. This function can be used only with IPv6. Therefore, if the host name with the IPv6 only defined is specified with hosts (host name information) in the SMTP server, the E-mail addressed to the said server is discarded.
3. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
4. When using e-mail messages and log e-mail simultaneously, do not set more than 1 entry for log e-mail destination address and 1 entry for SMTP server. If defined with more than 1 entry, e-mail transmissions may be delayed several minutes beyond the set time due to entry count and the load conditions of the SMTP server used for log e-mail and e-mail messages.

Downloaded from www.Manualslib.com manuals search engine

4.3 report (e-mail report information)

This sets information for the purpose of sending reports of failure information by e-mail. It is possible to set a maximum of 1 entry for local e-mail address, destination e-mail address and SMTP server information for sending e-mail reports.

Input Format

Setting information:

- Setting enable/disable

  ```
  [set] report [{ yes | no }]
  ```

- Setting local e-mail addresses

  ```
  [set] report email-from <E-Mail Address>
  ```

- Setting SMTP server information

  ```
  [set] report smtp { <Host Name> | <IP Address> } [-port <Port No.>]
  ```

- Setting destination e-mail addresses

  ```
  [set] report email assist <E-Mail Address> -manufacturing_number <Mfg No.>
  ```

Changing information:

- Setting enable/disable

  ```
  [set] report [{ yes | no }]
  ```

- Setting local e-mail addresses

  ```
  [set] report email-from <E-Mail Address>
  ```

- Setting SMTP server information

  ```
  [set] report smtp { <Host Name> | <IP Address> } [-port <Port No.>]
  ```

- Setting destination e-mail addresses

  ```
  [set] report email assist <E-Mail Address> -manufacturing_number <Mfg No.>
  ```

Deleting information:

```
delete report
delete report email-from
delete report smtp
delete report email assist
```

Display information:

```
show report
```

Parameter

`[ { yes | no } ]`

Description: Sets whether or not to use the e-mail report function

Default: yes ("no" is the default if e-mail report information is not set)

Range of value: yes or no

`email-from <E-Mail Address>`

Description: Specifies the local e-mail address

Downloaded from www.Manualslib.com manuals search engine

```
smtp { <Host Name> | <IP Address> }
```

Description: Specifies the SMTP server host name or IPv4 address for sending e-mail reports

```
[-port <Port No.>]
```

Description: Specifies the SMTP server port number for sending e-mail reports

Default: Standard value (25)

Range of value: 0 - 655535 (decimal). If set to 0, it operates at the standard value (25).

```
email assist
```

Specifies the e-mail destination maintenance service center. Our GR2000 Product Support Service (PSS) is used by specifying "assist."

```
<E-Mail Address>
```

Specifies the destination e-mail address

```
-manufacturing_number <Mfg No.>
```

Specifies the code that enables the e-mail destination maintenance service center to identify the reported device. The manufacturing number of the device is specified. Refer to Table 4-1, Location of appended manufacturing number seals, which are appended to the device in the locations indicated below.

Table 4-1 Location of appended manufacturing number seals

Model	Location of appended manufacturing number seals
GR2000-1B	Bottom of the device
GR2000-2B	Bottom of the device
GR2000-2B+	Bottom of the device
GR2000-BH	Bottom of the device
GR2000-2S	Lower right viewed from the front
GR2000-4S	Lower right viewed from the front
GR2000-6H	Lower right viewed from the front
GR2000-10H	Lower left of NIF board insertion surface
GR2000-20H	Lower left of RP board insertion surface
GR2000-4	Lower right viewed from the front
GR2000-10	Lower right of NIF board insertion surface
GR2000-20	Lower left of NIF board insertion surface

Downloaded from www.Manualslib.com manuals search engine

Example

1. Setting parameters
   The destination e-main address used for e-mail reports is set in nobody@router-1.mydomain.co.jp.

```
(config)# report email-from nobody@router-1.mydomain.co.jp
(config)# show report
report yes {
    email-from nobody@router-1.mydomain.co.jp;
};
(config)#
```

   - The SMTP server used for e-mail reports is set in loghost.

```
(config)# report smtp loghost
(config)# show report
report yes {
    email-from nobody@router-1.mydomain.co.jp;
    smtp loghost;
};
(config)#
```

   - Setting so that an e-mail report is sent to e-mail address logger@loghost by device manufacturing number 1234.

```
(config)# report email assist logger@loghost -manufacturing_number 1234
(config)# show report
report yes {
    email-from nobody@router-1.mydomain.co.jp;
    smtp loghost;
    email assist logger@loghost manufacturing_number 1234;
};
(config)#
```

2. Changing parameters
   Setting the SMTP server used for e-mail reports in loghost port number 10025.

```
(config)# report smtp loghost -port 10025
report yes {
    smtp loghost port 10025;
};
(config)#
```

   - Setting the SMTP server used for e-mail reports in the default value when the loghost port number is omitted

```
(config)# delete report smtp loghost -port
(config)#
```

3. Displaying parameters
   Displaying the settings.

```
(config)# show report
report yes {
    email-from nobody@router-1.mydomain.co.jp;
    smtp loghost;
    email assist logger@loghost manufacturing_number 1234;
};
(config)#
```

4. Deleting parameters
   Deleting destination e-mail address definitions.

```
(config)# delete report email assist
Are you sure? (y/n): y
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

- Deleting SMTP server definitions.

```
(config)# delete report smtp
Are you sure? (y/n): y
(config)#
```

- Deleting destination e-mail address definitions.

```
(config)# delete report email-from
Are you sure? (y/n): y
(config)#
```

- Deleting e-mail report definitions.

```
(config)# delete report
Are you sure? (y/n): y
(config)#
```

Related Configuration Object

hosts(Host name information)

dns-resolver(DNS resolver information)

Precautions

1. It is necessary to have a GR2000 Product Support Service (PSS) contract in order to us this function. Contact our sales department for information regarding PSS contracts. It is also necessary to connect the device to a network environment that enables e-mail transmissions via the Internet.
2. It is possible to set a maximum of 1 entry for local e-mail address, SMTP server and destination e-mail address.
3. When using e-mail reports, it is necessary to set the local e-mail address, SMTP server and destination e-mail address. Set, change or delete the destination e-mail address after setting the local e-mail address and SMTP server.
4. Confirm fully that the SMTP server settings (host name or IP address, port number) coincide with the SMTP settings of the connection destination. The message is discarded if the connection with the destination SMTP server fails when sending an e-mail report.
5. Confirm fully that the e-mail address settings coincide with the settings in the SMTP server definition. The message is discarded if the e-mail transmission fails.
6. This function is only usable with IPv4. Therefore, if a host name that only has an IPv6 address defined in the SMTP server by "hosts" (host name information) is specified, e-mail reports to the server destination is discarded.
7. Host name of this device must be predefined by dns_resolver hostname.
8. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
9. Do not set the local e-mail address that is set in the device in any other device on the network. If it is set, it may not be possible to send e-mail messages depending on the SMTP server, etc.
10. When using e-mail messages and log e-mail simultaneously, do not set more than 1 entry for log e-mail destination address and 1 entry for SMTP server. If defined with more than 1 entry, e-mail transmissions may be delayed several minutes beyond the set time due to entry count and the load conditions of the SMTP server used for log e-mail and e-mail messages.

Downloaded from www.Manualslib.com manuals search engine

11. Characters usable in e-mail addresses are limited to lower- and upper-case alphabet, numerals, hyphen (-), dot (.) and "at" sign (@). Note that underscoring cannot be used. In addition, the "@" sign cannot be used at the beginning or end of the address and no more than 1 can be used per address.
12. The e-mail address length is limited to a maximum of 255 characters. All characters beyond 255 are ignored if 256 or more characters are set.

Downloaded from www.Manualslib.com manuals search engine

4.4 NTP Object - *ntp*

Note: This object must be used in conjunction with the configuration subcommand.

Function

Object for creation, deletion, and display of the NTP configuration information, i.e., the router's timer setting information in synchronization with the NTP server.

Input Format

To create the NTP configuration information:

```
[set] ntp peer <address> [-key <key>] [-version { 1 | 2 | 3 }] [-prefer]
[set] ntp server <address> [-key <key>] [-version { 1 | 2 | 3 }] [-prefer]
[set] ntp broadcast <address> [-key <key>] [-version { 1 | 2 | 3 }]
[set] ntp -broadcastclient
[set] ntp trustedkey <key>
[set] ntp restrict <address> [-mask <mask>] [-ignore] [-noquery]
[-nomodify] [-noserve] [-nopeer] [-notrust] [-limited] [-ntpport]
[set] ntp -clientlimit <limit>
[set] ntp -master [-stratum <int>]
[set] ntp -broadcastdelay <seconds>
[set] ntp -authenticate
[set] ntp authentication-key <key> -md5 <value>
```

To delete the NTP configuration information:

```
delete ntp peer <address>
delete ntp server <address>
delete ntp broadcast <address>
delete ntp trustedkey <key>
delete ntp authentication-key <key>
```

To show the NTP configuration information:

```
show ntp
```

Parameter

```
peer <IP Address> [-key <key>] [-version { 1 | 2 | 3 }] [-prefer]
```

This set of parameters specifies the peer server.

<address>

Description:	Specifies the IP address of the target server as a peer server.
Default:	Undefined (mandatory input).
Range of Value:	IP address in dot notation or host name defined with `hosts` object.

Downloaded from www.Manualslib.com manuals search engine

`-key <key>`

Description: Specifies the authentication key number used for accessing the peer server. The key number must be the one defined by the `authentication-key` parameter.

Default: No authentication key.

Range of Value: 1–4294967295 in decimal.

`-version { 1 | 2 | 3 }`

Description: Specifies the NTP version.

Default: 3

Range of Value: 1, 2, or 3

`-prefer`

Description: Grants privilege to the subject peer server among multiple peer servers defined.

Default: No privilege

`server <IP Address> [-key <key>] [-version { 1 | 2 | 3 }] [-prefer]`

Description: This set of parameters specifies the time server.

`<IP Address>`

Description: Specifies the IP address of the target server as a time server.

Default: Undefined (mandatory input)

Range of Value: IP address in dot notation or host name defined with `hosts` object.

`-key <key>`

Description: Specifies the authentication key number used for accessing the time server. The key number must be the one defined by the `authentication-key` parameter.

Default: No authentication key

Range of Value: 1–4294967295 in decimal

`-version { 1 | 2 | 3 }`

Description: Specifies the NTP version

Default: 3

Range of Value: 1, 2, or 3

`-prefer`

Description: Grants privilege to the subject time server among multiple time servers defined.

Default: No privilege

Downloaded from www.Manualslib.com manuals search engine

```
broadcast <IP Address> [-key <key>] [-version { 1 | 2 | 3 }]
```

Description: This set of parameters specifies transmission of the NTP packet in broadcast or multicast connection. The NTP packet transmission in multicast connection is supported in version 02-01 or above.

`<IP Address>`

Description: Specifies the broadcast or multicast IP address

Default: Undefined (mandatory input)

Range of Value: IP address in dot notation

`-key <key>`

Description: Specifies the authentication key number. The key number must be the one defined by the `authentication-key` parameter.

Default: No authentication key

Range of Value: 1–4294967295 in decimal

`-version { 1 | 2 | 3 }`

Description: Specifies the NTP version

Default: 3

Range of Value: 1, 2, or 3

`-broadcastclient`

Description: Specifies receipt of an ntp broadcast message sent from the time server connected on the subnet.

Default: No receipt

`trustedkey <key>`

Description: Specifies the authentication key number. The key number must be the one defined by the `authentication-key` parameter.

Default: No authentication key

Range of Value: (`<key>`): 1–4294967295 in decimal

```
restrict <IP Address> [-mask <mask>] [-ignore] [-noquery] [-nomodify]
[-noserve] [-nopeer] [-notrust] [-limited] [-ntpport]
```

Description: This set of parameters specifies the address used in limiting access to the local NTP server.

`<IP Address>`

Description: Specifies the access-limiting address or the subnet address.

Default: Undefined (mandatory input).

Range of Value: IP address in dot notation.

Downloaded from www.Manualslib.com manuals search engine

`<mask>`

Description: Specifies the net mask address

Default: No mask

Range of Value: Net mask address in dot notation

`-ignore -noquery -nomodify -noserve -nopeer -notrust -limited -ntpport`

Description: These parameters, if specified, execute actions below.

`-ignore` Ignores all accesses from the specified host.

`-noquery` Ignores all the NTP Mode 6 and Mode 7 packets sent from the specified source. Time service with that source continues.

`-nomodify` Allows only referential access from the specified host, using the NTP Mode 6 and Mode 7 packets.

`-noserve` Ignores packets from the specified host other than those of Mode 6 and Mode 7. As a result, no time service is given to that host.

`-nopeer` Treats the specified host not as a peer.

`-notrust` Treats the specified host not as a server for time data synchronization.

`-limited` Accepts only the first-issued time data request from a client belonging to the specified net. Any other time data request issued later from the other clients of the specified net is rejected in accordance with the `clientlimit` parameter setting.

`-ntpport` Accepts only the packets issued from the NTP port.

Default: When none of the above parameters are specified, "`-ignore -ntpport`" is assumed by default.

`-clientlimit <limit>`

Description: Specifies the maximum number of clients that can access the same NTP server at a time per network.

Default: 3

Range of Value: (`<key>`): 1–4294967295 in decimal

`-master [-stratum <int>]`

Description: Specifies the local time server definition and the stratum setting. This definition applies when no remote time server exists in the network to which the router ordinarily connects.

Default: On with the stratum setting of 8.

Range of Value: (`<int>`): 1–255 in decimal.

`-broadcastdelay <seconds>`

Description: Specifies the delay time in seconds with which a broadcast or multicast packet arrives.

Default: 0.004 when no value is specified

Range of Value: Less than 1 in fixed-point decimal

Downloaded from www.Manualslib.com manuals search engine

`-authenticate`

Description: Enables the authentication key definition

Default: Off

`authentication-key <key> -md5 <value>`

Description: Defines the authentication key

Default: No authentication key

Range of value:

<key> 1–4294967295 in decimal

<value> Up to 30 ASCII characters.

Example

Define an NTP server with the IP address 192.168.1.100:

```
(config)#  ntp server 192.168.1.100
(config)# show ntp
ntp{
  server 192.168.1.100;
};
(config)#
```

Define peer servers and show the result:

```
(config)#  ntp server 192.168.1.4
(config)#  ntp server 192.168.1.5
(config)#  show ntp
ntp {
    server 192.168.1.4;
    server 192.168.1.5;
};
(config)#
```

Delete one of the defined peer servers:

```
(config)# show ntp
ntp {
server 192.168.1.4;
    server 192.168.1.5;
};
(config)# delete ntp server 192.168.1.4
(config)# show ntp
ntp {
    server 192.168.1.5;
};
(config)#
```

Related Configuration Object

`ntp`

Downloaded from www.Manualslib.com manuals search engine

Related Standards

The NTP specifications of GR2000 are based on RFC1305.

Precautions

- Depending on the type of the connected NTP server, the usable authentication key length may be shorter than 32 bits. In such a case, adjust the key contents to match the usable key length of the connected NTP server.
- If a host name is specified to the <address> parameter where applicable (e.g., peer, server, and broadcast) and such host name is wrong, no error checking will be performed. Once the definition operation is complete, make sure that the host name specified with this object is displayed on the console. Incidentally, if a host name is initially specified with this ntp object and thereafter another host name is added with the hosts object, the change does not promptly take effect. To force the change to take effect, restart the NTP server with the command string *GR2000 Operations Commands, Vol. 1*, restart ntp command.
- If the difference of internal clocks between the referenced server and this GR2000 router is 1000 seconds (approx. 16 minutes) or more, the time data synchronization does not take place because the server is regarded as invalid. If the server's time (i.e., the time of the host containing the time server to which this router references as the time source) turns out to be correct, then adjust the router's time to the server's time using *GR2000 Operations Commands, Vol. 1*, set calendar or rdate command.
- In a configuration where this router references multiple time servers and any time difference among the time servers is 16 seconds or more, this router can synchronize with its time servers but devices subordinately connected to this router cannot synchronize with this router acting as their time server. In such a case, make sure that the said configuration is as expected and see if the time settings of the defined time servers are correct.
- When this router and multiple time servers employ peer-to-peer connections, there may be cases when a very long time is required before this router completes time synchronization with all these time servers. If this could happen, it is recommended to decrease the number of peers.
- When this router refers to multiple time servers and one time server fails to provide time data within the allowable range (less than 1000 seconds), the server for the time synchronization target automatically switches to any other server available. If such occurrence is left without an appropriate action, however, the synchronization target will be eventually disconnected. To avoid this, you must disable the router's referencing the failing time server. Incidentally, while the said synchronization is off and the failing time server setting is adjusted to fall within the allowable range, the synchronization with the time server is automatically recovered.
- This function can be used only with IPv6. Therefore, if the host name with the IPv6 only defined is specified with hosts (host name information) in the peer server, the peer server is nullified.
- If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.
- If using this device as NTP server, set the number of synchronized clients at a maximum of 10.

Downloaded from www.Manualslib.com manuals search engine

- If the IP address of the device is set by "config router local-address," the IP address of the device is used as the local IP address when sending NTP packets. Therefore, if the device is set as NTP server or peer, specify the IP address of the device as the IP address. When adding, changing or deleting device IP addresses, reinitialize the ntp program using the "restart ntp" command.
- When using MPLS, the MPLS function stops when the time reverts by the NTP function. In addition, the "copy running-config" command and changes in configuration definitions will not operate properly. If this happens, reboot the MPLS program using the "restart mpls" command. [ROUTE-OS7]

Downloaded from www.Manualslib.com manuals search engine

4.5 radius (RADIUS server information)

The following is an explanation of configuration definition commands and parameters that define information for the purpose of controlling GR2000 access using RADIUS authentication.

This sets RADIUS servers used for authentication.

Input Format

Setting information:

Setting RADIUS server information

```
[set] radius {<IPv4 Address>|<Host Name>} -key <Strings> [-auth_port
<Port No.>] [-primary]
```

Setting RADIUS connection information

```
[set] radius [{yes|no}] [-retransmit <Count>] [-timeout <Seconds>]
```

Changing information:

Changing RADIUS server information

```
[set] radius {<IPv4 Address>|<Host Name>} [-key <Strings>]
[-auth_port <Port No.>] [-primary]
```

Changing RADIUS connection information

```
[set] radius [{yes|no}] [-retransmit <Counts>] [-timeout <Seconds>]
```

Deleting information

```
delete radius {<IPv4 Address> | <Host Name>}
```

Display information

```
show radius
```

Parameter

`{<IPv4 Address> | <Host Name>}`

Description: Specifies the RADIUS server IPv4 address or host name.

Default: None

Range of Value: IPv4 address (dot notation) or host name is specified.

`-key <Strings>`

Description: Specifies the RADIUS key used in encryption and authentication of communication between RADIUS servers. It is necessary to set the same RADIUS key in clients and in RADIUS servers.

Default: None

Range of Value: A character string of a password exceeding one character and not exceeding 64 characters is set using double quotation marks ("). Alphanumeric characters and special characters can be entered. However, a character string can be entered without using double quotation marks (") when no special character (e.g., space) is contained in an entry character string. However, notice that the characters below cannot be used.

Downloaded from www.Manualslib.com manuals search engine

"(double quotation mark), { (beginning of brace), } (end of brace), ' (single quotation mark), ; (semicolon), $ (dollar), and ' (reverse single quotation mark).

For more information, see Table 1-95

`-auth_port <Port No.>`

Description: Specifies the RADIUS server port number.

Default: Uses port number 1812.

Range of Value: 0 - 65535

`-primary`

Description: Used the specified RADIUS server with priority.
The RADIUS server specifying the "primary" option is used first for authentication. If the "primary" option is used for multiple RADIUS servers, the RADIUS server specified as "primary" and highest in the display of configuration definition information is used.

Default: Priority is not set.

Range of Value: None

`-retransmit <Counts.>`

Description: Specifies the number of authentication demands resent to RADIUS servers.

Default: 2 (times).

Range of Value: 0 - 15

`-timeout <Seconds>`

Description: Specifies the timeout time for a response from RADIUS servers.

Default: 5 (sec).

Range of Value: 1 - 30

Example

1. Specifying RADIUS servers:
   Setting IP address 192.168.10.1, RADIUS key "Aodiug-cl3*%63j9d" and the RADIUS server.

```
(config)# radius yes
(config)# radius 192.168.10.1 -key "Aodiug-cl3*%63j9d"
(config)# show radius
radius yes {
    192.168.10.1 {
        key "Aodiug-cl3*%63j9d" ;
    };
};
```


Downloaded from www.Manualslib.com manuals search engine

- Setting IP address 172.16.100.1 and RADIUS key "Okdf8dL#LIdjei87+e" as the second RADIUS server.

```
(config)# radius 172.16.100.1 -key "Okdf8dL#LIdjei87+e"
(config)# show radius
radius yes {
    192.168.10.1 {
        key "Aodiug-cl3*%63j9d";
    };
    172.16.100.1 {
        key "Okdf8dL#LIdjei87+e";
    };
};
```

2. Adding parameters:
   Setting resend count 3 and timeout time 10 seconds as RADIUS connection information.

```
(config)# radius -retransmit 3 -timeout 10
(config)# show radius
radius yes {
    192.168.10.1 {
        key "Aodiug-cl3*%63j9d";
    };
    172.16.100.1 {
        key "Okdf8dL#LIdjei87+e";
    };
    retransmit 3;
    timeout 10;
};
```

- Specifying 1645 as RADIUS server port number of IP address 192.168.10.1 and to use RADIUS server at IP address 172.16.100.1 first when initiating authentication.

```
(config)# radius 192.168.10.1 -auth_port 1645
(config)# radius 172.16.100.1 -primary
(config)# show radius
radius yes {
    192.168.10.1 {
        key "Aodiug-cl3*%63j9d";
        auth_port 1645;
    };
    172.16.100.1 {
        key "Okdf8dL#LIdjei87+e";
        primary;
    };
    retransmit 3;
    timeout 10;
};
```

3. Changing parameters:
   Changing the authentication key of RADIUS server at IP address 192.168.10.1 to "DIT974J?FIR63KKDIEKSW6."

```
(config)# radius 192.168.10.1 -key "DIT974J?FIR63KKDIEKSW6"
(config)# show radius
radius yes {
    192.168.10.1 {
        key "DIT974J?FIR63KKDIEKSW6";
        auth_port 1645;
    };
    172.16.100.1 {
        key "Okdf8dL#LIdjei87+e";
        primary;
    };
    retransmit 3;
    timeout 10;
};
```


Downloaded from www.Manualslib.com manuals search engine

4. Deleting parameters:
   Deleting the RADIUS server port number of IP address 192.168.10.1 and reverting to the default value.

```
(config)# radius 192.168.10.1 --auth_port
(config)# show radius
radius yes {
    192.168.10.1 {
        key "DIT974J?FIR63KKDIEKSW6";
    };
    172.16.100.1 {
        key "Okdf8dL#LIdjei87+e";
        primary;
    };
    retransmit 3;
    timeout 10;
};
```

   - Deleting the resend count designation in RADIUS connection information.

```
(config)# radius --retransmit
(config)# show radius
radius yes {
    192.168.10.1 {
        key "DIT974J?FIR63KKDIEKSW6";
    };
    172.16.100.1 {
        key "Okdf8dL#LIdjei87+e";
        primary;
    };
    timeout 10;
};
```

5. Deleting RADIUS servers
   Deleting the RADIUS server of IP address 172.16.100.1.

```
(config)# delete radius 172.16.100.1
(config)# show radius
radius yes {
    192.168.10.1 {
        key "Aodiug-cl3*%63j9d";
    };
    timeout 10;
};
```

   - Deleting all RADIUS information.

```
(config)# delete radius
(config)# show radius
no such radius
```

Related Configuration Object

```
router
```

Precautions

1. There is a maximum of 4 settable RADIUS servers per device.

Downloaded from www.Manualslib.com manuals search engine

4.6 Board Disablement Object - *disable*

Note: This object must be used in conjunction with the configuration subcommand.

Function

Object for creation, deletion, and display of the board disablement definition. You can set and alter configuration information on lines accommodated in the disabled NIF, regardless of the NIF type.

Input Format

To create board disablement definition:

```
[set] disable [ rp <RP.No> | nif <NIF.No> ]
```

To delete board disablement definition:

```
delete disable [ rp <RP.No> | nif <NIF.No> ]
```

To show board disablement definition:

```
show disable
```

Parameter

```
rp <RP.No> | nif <NIF.No>
```

Description: Defines disablement of the RP board with the specified RP number or the NIF board with the specified NIF number.

Example

Create board disablement definition and show the result:

```
(config)#  disable rp 1
(config)#  show disable
(config)#
```

Delete board disablement definition:

```
(config)#  delete disable rp 1
Are you sure?  (y/n):y
(config)#
```

Displaying the configuration information
To show the disable information.

```
(config)# show disable
disable {
        rp 1;
};
(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Configuration Object

None

Precautions

- The board slot defined as disabled with the `disable` object is not restarted even when the upper hardware is re-initialized. Such board slot is not restarted with the free command (refer to the *GR2000 Operations Commands, Vol. 1*. To unlock the status, you must delete the disablement definition.
- Whether any hardware has disablement definition or not can be confirmed by the show router command or the MIB gr2kRpOperStatus in *GR2000 Operations Commands, Vol. 1*.
- If the set command with the `disable` object has been executed on an NIF for OC-3c/STM ATM 1or an RP with such NIF installed, the T/R LED indicator for data transmission turns on. This is not an error and the command execution ends normally.
- If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

4.7 Default Configuration Objects

4.7.1 *default*

Function

Sets the configuration to the user-defined default values with the set subcommand, or displays the default values for the configuration with the show subcommand.

Input Format

To display the default values for the configuration information:

```
show default
```

Parameter

Following displays a list of items and the parameters supported, which can be set to be used as it's initial default values.

Example

Customize the default settings for SNMP and frame relay PVC status notification and display the results:

```
(config)# default -snmp_read
(config)# show default
default {
    snmp_read;
};
(config)#

(config)# default -frame_relay_poll_direction dte
default {
    snmp_read;
    frame_relay_poll_direction dte;
};
(config)#
(config)#
```

Related Configuration Object

None

Precautions

1. You cannot directly customize the default settings of a configuration in use. In order to customize the default settings of the configuration, create a new configuration file using the copy subcommand, edit the new configuration, and replace the configuration with the edited file using the copy subcommand again.
2. If this command is inputted in the cases where changes are made on the IP routing protocol information, the IP multicast protocol information, and the MPLS information, and the apply command is not being executed, the apply subcommand is executed before the command is executed, and the changed IP routing protocol information, IP multicast routing protocol information, and MPLS information are reflected to the operation.

Downloaded from www.Manualslib.com manuals search engine

4.7.2 SNMP Information

Input Format

```
[set]  default
   [ { -snmp_read | -snmp_read_write } ]
   [ { -snmp_none | -snmp_trap | -snmp_ex_trap | snmp_selection_trap } ]
   [ -snmp_level <No.> ]
   [ -snmp_trap_version { 1 | 2 } ]
   [ -snmp_system_msg_trap_level<No.> ]
   [ { -snmp_limited_coldstart_trap | -snmp_unlimited_coldstart_trap } ]
   [ -snmp_link_trap_mode {protocol | interface} ]
   [ -rmon_history_control_buckets_requested <Number> ]
   [ -rmon_history_control_interval <Number> ]
   [ -rmon_alarm_startup_alarm { rising_falling | rising | falling } ]
   [-snmp_link_trap_bind_info {private | standard}]
```

Parameters

The initial value items that can be set using SNMP information and the initial values during initial installation are shown in Table 4-2. For details of each parameter, refer to the configuration definition information in "Section 3.1, “SNMP Objects".

Table 4-2 List of Initial Value Items that Can Be Set Using SNMP Information and Initial Values during Initial Installation

Information Group Name	Information Name	Initial Value
SNMP information	Reference mode of MIB information	Only the reference of MIB information is enabled. (Read)
	Trap transmission mode	Not transmitted. (None)
	Transmission level of system message Trap	System message Trap for a fatal failure is transmitted. (Level 9)
	Selection of Trap version	Version 1
	Transmission level of system message Trap during trap selection	System message Trap for fatal failure (Level 9)
	Limited moment of coldStart trap issuing	The moment at which coldStart trap is issued is not limited. (limited_coldstart_trap)
	Number of log entries in which RMON static information is stored	50 entries
	Time interval at which RMON static information is collected	Static information is collected at intervals of 30 minutes.
	Timing in which RMON threshold check starts	An alarm is generated when the upward or downward threshold value is exceeded during first sampling. (rising&falling)
	Limited moment of link trap issuing	The moment at which link trap is issued is not limited. (protocol)
	Selection of link trap appended information	When link traps are issued, it is information that appends MIBS that comply with RFC (standard)

Downloaded from www.Manualslib.com manuals search engine

4.7.3 Line Information (Ethernet/Gibabit Ethernet)

Input Format

```
[set]  default
   [ -ethernet_type { auto_negotiation | 10m_ethernet | 10m_full_deplex |
   100m_half_deplex | 100m_full_duplex } ]
   [ -ethernet_tpid_9100 ]
   [ { -gigabit_ethernet_flow_control | -gigabit_ethernet_flow_control_off}]
   [ -gigabit_ethernet_mtu { 1500 | 1488 }]
   [ -gigabit_ethernet_type { 1000m_full_duplex | auto_negotiation }]
   [ -gigabit_ethernet_tpid_9100 ]
```

Parameters

The initial value items that can be set using line Information (Ethernet/Gibabit Ethernet) and the initial values during initial installation are shown in Table 4-3. For details of each parameter, refer to the configuration definition information in "line Information (Ethernet/Gibabit Ethernet)."

Table 4-3 List of Initial Value Items that Can Be Set Using line Information (Ethernet / Gigabit Ethernet) and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
line Information (Ethernet / Gigabit Ethernet)	Segment standard of 10BASE-T and 100BASE-TX	Automatic recognition (auto negotiation)
	Flow control function option in 1000BASE-LX, 1000BASE-SX, and 100BASE-LH	Enable
	MTU length of 1000BASE-LX, 1000BASE-SX, and 100BASE-LH	1500 bytes
	Segment standard of 1000BASE-LX, 1000BASE-SX, and 100BASE-LH	1000M full-duplex
	10BASE-T, 100BASE-TX, 1000BASE-LX, 1000BASE-SX, TPID option in 100BASE-LH	0x8100

Downloaded from www.Manualslib.com manuals search engine

4.7.4 Line Information (WAN)

Input Format

```
[set]  default
   [ -e1_frame_format { crc4 | no_crc4 } ]
   [ -e1_line_code { ami | hdb3 } ]
   [ -e1_clock { external | independent } ]
   [ -e1_national_bit_g704 <Pattern> ]
   [ -e1_timeslot_speed { 56 | 64 } ]
   [ -t3_clock { external | independent } ]
   [ -t3_crc { 16 | 32 } ]
   [ { -t3_scramble | -t3_scramble_off } ]
   [ -t3_location { ci | carrier } ]
   [ -t3_remote_loopback { payload Åb line | disable } ]
   [ -t3_mdl { pid | tsid | isid | disable } ]
   [ -t1_frame_format { esf | sf } ]
   [ -t1_line_code { ami | b8zs } ]
   [ -t1_clock { external | independent } ]
   [ -t1_timeslot_speed { 56 | 64 } ]
   [ -t1_location { ci | carrier } ]
   [ -t1_data_link { ansi | att | bellcore } ]
   [ -t1_remote_loopback { auto | disable } ]
   [ -t1_prm { enable | disable } ]
   [ -e3_clock { external | independent } ]
   [ -e3_national_bit_g751 <Pattern> ]
   [ -e3_crc { 16 | 32 } ]
   [ {-e3_scramble | -e3_scramble_off } ]
   [ -ce3_clock { external | independent } ]
   [ -ce3_national_bit_g751 <Pattern> ]
   [ -ce3_crc {16 | 32}]
   [ -ct3_frame_format { cbit | m23 } ]
   [ -ct3_clock { external | independent } ]
   [ -ct3_crc {16 | 32}]
```

Parameters

The initial value items that can be set using line Information (WAN) and the initial values during initial installation are shown in Table 4-4. For details of each parameter, refer to the configuration definition information in "line (line Information), Serial/OC-3c(POS)/ OC-12c(POS)/ OC-48(POS)/ BRI(leased line)/ PRI(leased line)/ J2/ BRI (ISDN)/ PRI (ISDN)/ T1 (leased line)/ E1 (leased line)/ T3 non-multiplex (leased line)/ E3 non-multiplex (leased line)/ E3 multiplex (leased line)".

Downloaded from www.Manualslib.com manuals search engine

Table 4-4 List of Initial Value Items that Can Be Set Using line Information (WAN) and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
line Information (WAN)	Selection of physical layer frame format in E1	CRC-4 Multiframe (crc4)
	Selection of physical layer line code format in E1	HDB3(High Density Bipolar 3)(hdb3)
	Selection of synchronized clock in E1	Synchronized with the received clock. (external)
	Setting value of national bit in E1	0 (hexadecimal) (2^7: SI, 2^6: Unused, 2^5: Unused, 2^4: SA-4, 2^3: SA-5, 2^2: SA-6, 2^1: SA-7, 2^0: SA-8)
	Selection of timeslot line rate in E1	64 kbps (64)
	Selection of synchronized clocks in T3	Synchronized with the clock in a local router. (independent)
	CRC length in T3	16 (bits)
	Selection of scramble disable/enable in T3	Disable (-t3_scramble_off)
	Selection of installation position in T3 network	CI(Customer Installation) (ci)
	Selection of acceptance during remote loop-back test request in T3	The remote loop-back test request can be accepted. The loop-back type specifies payload loop-back. (payload)
	Selection of MDL message in T3	MDL stops. (disable)
	Selection of physical layer frame format in T1	ESF(Extended Superframe) (esf)
	Selection of physical layer line code format in T1	B8ZS (Bipolar with 8 Zeros Substitutions) (b8zs)
	Selection of synchronized clock in T1	Synchronized with the received clock. (external)
	Selection of timeslot line rate I T1	64 kbps (64)
	Selection of installation position in T1 network	CI(Customer Installation) (ci)
	Selection of FDL type in T1	AVSI T1.403(ansi)
	Selection of acceptance during remote loop-back test request in T1	The remote loop-back test request can be accepted. (auto)
	Selection of PRM transmission/response in T1	The PRM transmission/response is enabled. (enable)
	Selection of synchronized clock in E3	Synchronized with the received clock. (external)
	Setting value of national bit in E3	0 (Na = 0)
	CRC length in E3	16 (bits)
	Selection of scramble disable/enable in E3	Disable (-e3_scramble_off)
line Information (WAN) (continued)	Selection of synchronized multi-clock in E3	Synchronized with the received clock. (external)
	Setting value of national multi-bit in E3	0 (Na = 0)
	Multi-CRC length in E3	16 (bits)
	Selection of physical layer multi-frame format in E3	C-bit parity frame (cbit)
	Selection of synchronized multi-clock in T3	Synchronized with the clock in a local router. (independent)
	Multi-CRC length in T3	16 (bits)

Downloaded from www.Manualslib.com manuals search engine

4.7.5 Line Information (WAN OC-POS)

Input Format

```
[set]  default
    [ -oc3pos_clock { external | independent } ]
    [ -oc3pos_crc { 16 | 32 } ]
    [ { -oc3pos_scramble | -oc3pos_scramble_off } ]
    [ -oc3pos_sonet_overhead <Pattern> ]
    [ -oc12pos_clock { external | independent } ]
    [ -oc12pos_crc { 16 | 32 } ]
    [ { -oc12pos_scramble | -oc12pos_scramble_off } ]
    [ -oc12pos_sonet_overhead <Pattern> ]
    [ -oc48pos_clock { external | independent } ]
    [ -oc48pos_crc { 16 | 32 } ]
    [ {-oc48pos_scramble | -oc48pos_scramble_off } ]
    [ -oc48pos_sonet_overhead <Pattern> ]
    [ -oc48pos_mode { sdh | sonet | japanese_local } ]
    [ { -oc48pos_aps | -oc48pos_aps_off } ]
    [ -oc48pos_wait_to_restore_time <Time> ]
    [ -oc48pos_aps_protocol { bellcore_gr253_1+1 | jt_g783_annex_b } ]
    [ { -oc48pos_unidirectional | -oc48pos_bidirectional } ]
    [ { -oc48pos_revertive | -oc48pos_non_revertive } ]
    [ -oc48pos_sd_ber <ErrorRate> ]
    [ -oc48pos_sf_ber <ErrorRate> ]
```

Parameters

The initial value items that can be set using line Information (WAN OC-POS) and the initial values during initial installation are shown in Table 4-5. For details of each parameter, refer to the configuration definition information in "line (line Information) Serial/OC-3c(POS)/ OC-12c(POS)/ OC-48(POS)/ BRI(leased line)/ PRI(leased line)/ J2/ BRI (ISDN)/ PRI (ISDN)/ T1 (leased line)/ E1 (leased line)/ T3 non-multiplex (leased line)/ E3 non-multiplex (leased line)/ E3 multiplex (leased line)".".

Downloaded from www.Manualslib.com manuals search engine

Table 4-5 List of Initial Value Items that Can Be Set Using line Information (WAN OC-POS) and Initial Values during Initial Installation

Information Group Name	Information Name	Initial Value
line Information (WAN OC-POS)	Selection of synchronized clocks in oc3pos	Synchronized with the clock in a local router. (independent)
	Multi-CRC length in oc3pos	16 (bits)
	Selection of scramble disable/enable in oc3pos	Disable (oc3pos_scramble_off)
	Setting value of SONET overhead in oc3pos	Refer to *GR2000 Configuration Commands, (universal CLI) Vol. 1,* Setting Contents of SONET Overhead for the CF010000 (hexadecimal) value.
	Selection of synchronized clocks in oc12pos	Synchronized with the clock in a local router. (independent)
	Multi-CRC length in oc12pos	16 (bits)
	Selection of scramble disable/enable in oc12pos	Disable (oc12pos_scramble_off)
	Setting value of SONET overhead in oc12pos	Refer to *GR2000 Configuration Commands, (universal CLI) Vol. 1*, Setting Contents of SONET Overhead for the CF010000 (hexadecimal) value.
	Selection of synchronized clocks in oc48pos	Synchronized with the clock in a local router. (independent)
	Multi-CRC length in oc48pos	16 (bits)
	Selection of scramble disable/enable in oc48pos	Disable (oc48pos_scramble_off)
	Setting value of SONET overhead in oc48pos	Refer to *GR2000 Configuration Commands, (universal CLI) Vol. 1*, Setting Contents of SONET Overhead for the CF010000 (hexadecimal) value.
	Line operating mode in oc48POS	Sonet
	APS mode in oc48POS	APS is not used. (oc48pos_aps_off)
	APS return waiting time in oc48POS	300 (seconds)
	APS protocol type in oc48POS	JT-G783 Annex B (jt_g783_annex_b)
	APS switchover direction in oc48POS	Bidirectional switching (oc48pos_bidirectional)
	APS return mode in oc48POS	Non-return mode (oc48pos_non_revertive)
	SD BER threshold value in oc48POS	6
	SD BER threshold value in oc48POS	3

Downloaded from www.Manualslib.com manuals search engine

4.7.6 line Information (ATM)

Input Format

```
[set]  default
    [ -oc3atm_clock { external | independent } ]
    [ -oc3atm_frame_format { sdh_idle | sdh_unassigned | sonet_unassigned } ]
    [ -oc3atm_pvc_trap_interval <Interval>]
    [ -oc12atm_clock { external | independent } ]
    [ -oc12atm_frame_format { sdh_idle | sdh_unassigned | sonet_unassigned } ]
    [ -oc12atm_pvc_trap_interval <Interval>]
    [ -25atm_pvc_trap_interval <Interval>]
```

Parameters

The initial value items that can be set using line Information (ATM) and the initial values during initial installation are shown in Table 4-6. For details of each parameter, refer to the configuration definition information in "line (line Information) 25Mbps ATM/ OC-12c ATM".

Table 4-6 List of Initial Values That Can Be Set Using Line Information (ATM Information) and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
line Information (ATM)	Selection of clock in OC-3c ATM Line	external (External synchronization)
	Physical layer frame format and empty cell format in OC-3c ATM Line	sdh_idle (Physical layer frame format: SDH(STM-1, STM-4), empty cell format: ITU-T specifications)
	Transmission interval of ATM PVC Trap in OC-3c ATM Line	30 seconds
	Selection of clock in OC-12c ATM Line	external (External synchronization)
	Physical frame format and empty cell format in OC-12c ATM Line	sdh_idle (Physical layer frame format: SDH(STM-1, STM-4), empty cell format: ITU-T specifications)
	Transmission interval of ATM PVC Trap in OC-12c ATM Line	30 seconds
	Transmission interval of ATM PVC Trap in 25M ATM Line	30 seconds

Downloaded from www.Manualslib.com manuals search engine

4.7.7 Subline Information (WAN)

Input Format

```
[set]  default
   [-subline_el_frame_format {crc4 | no_crc4} ]
   [-subline_el_national_bit_g704 <Pattern> ]
   [-subline_el_timeslot_speed {56 | 64}]
   [-subline_tl_frame_format { esf | sf } ]
   [-subline_tl_timeslot_speed {56 | 64}]
```

Parameters

The initial value items that can be set using subline Information (WAN) and the initial values during initial installation are shown in Table 4-7. For details of each parameter, refer to the configuration definition information in "subline (subline Information)."

Table 4-7 List of Initial Values That Can Be Set Using Subline Information (WAN Line) and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
Subline information (WAN line)	Selection of E1 physical layer multi-frame format in E3	CRC-4 Multiframe (crc4)
	Setting value of E1 national multi-bit in E3	0 (hexadecimal) (2^7: SI, 2^6: Unused, 2^5: Unused, 2^4: SA-4, 2^3: SA-5, 2^2: SA-6, 2^1: SA-7, 2^0: SA-8)
	Selection of E1 timeslot multi-line rate in E3	64 kbps (64)
	Selection of T1 physical layer multi-frame format in T3	ESF (Extended Superframe) (esf)
	Selection of T1 timeslot multi-line rate in T3	64 kbps (64)

Downloaded from www.Manualslib.com manuals search engine

4.7.8 PPP Information

Input Format

```
[set]  default
    [ -ppp_source_mru <Bytes> ]
    [ -ppp_echo_trial_times <Count> ]
    [ -ppp_echo_success_times <Count> ]
    [ -ppp_echo_interval <Second> ]
    [ { -ppp_ip_address_negotiation_off | -ppp_ip_address_negotiation } ]
    [ -ppp_remote_ip_address_mode { assign | check } ]
    [ { -ppp_ipx_address_negotiation_off | -ppp_ipx_address_negotiation } ]
    [ { -ppp_ipv6cp_off | -ppp_ipv6cp } ]
```

Parameters

The initial value items that can be set using PPP Information and the initial values during initial installation are shown in Table 4-8. For details of each parameter, refer to the configuration definition information in "PPP Information".

Table 4-8 List of Initial Values that Can Be Set Using PPP Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
PPP information	Maximum data length that can be received using PPP protocol (Maximum value of MTU length in remote router)	4500 bytes
	Number of Echo-RQ frame retries using PPP protocol (Link quality monitoring function)	7 times
	Number of Echo-Reply reception times for judging a high-quality link using PPP protocol (Link quality monitoring function)	6 times
	Echo-RQ transmission interval using PPP protocol (Link quality monitoring function)	3 seconds
	Report of local address to the remote router using PPP protocol	Not reported.
	Operation when the remote router reports IP address using PPP protocol by IP address negotiation	A correct IP address is distributed as an IP address distribution request (assign).
	Report of local IPX node number to the remote router using PPP protocol	Not reported.
	Selection of IPV6CP used or not used by PPP protocol	Used.

Downloaded from www.Manualslib.com manuals search engine

4.7.9 PPPoE Information

Input Format

```
[set]  default
[-pppoe_authentication_protocol {pap | chap | auto}]
[-pppoe_echo_trial_times <Count>]
[-pppoe_echo_interval <Second>]
[-pppoe_auto_connection <Second>]
[-pppoe_dns {no | yes}]
[-pppoe_mru <Bytes>]
[-pppoe_mss {off | auto | <Bytes>}]
```

Parameters

TThe initial value items that can be set using PPP Information and the initial values during initial installation are shown in Table 4-9. For details of each parameter, refer to the configuration definition information in "PPPoE Information" [ROUTE-OS6B].

Table 4-9 List of Initial Values That Can Be Set Using PPPoE Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
PPPoE information	Certification protocol type used when connecting with a provider.	4500 bytes
	Number of echo-RQ frame trial (PPPoE session connection surveillance function)	5 times
	Interval of echo-RQ frame transmission (PPPoE session connection surveillance function)	60 second
	Automatic reconnection time for PPPoE session	10 seconds
	Designation of automatic acquisition of DNS server address	yes
	Maximum length of data that can be received in a PPPoE session. (Maximum value of MTU of the counterpart server)	1492 bytes
	Rewriting the maximum segment length (MSS) designation option of the TCP connection request (SYN) packet.	auto

Downloaded from www.Manualslib.com manuals search engine

4.7.10 Frame Relay Information

Input Format

```
[set]  default
   [ -frame_relay_local_management { q933 | no } ]
   [ -frame_relay_poll_direction { dte | dce | both } ]
   [ { -frame_relay_provide_single_pvc_status_off |
   -frame_relay_provide_single_pvc_status } ]
   [ -frame_relay_no_pvc_detection <Seconds> ]
   [ -frame_relay_cllm_sustain { no | <Seconds> } ]
   [ -frame_relay_max_packet_size <Bytes> ]
   [ { -dlci_drop | -dlci_forward } ]
   [ -dlci_max_packet_size <Bytes> ]
   [ -dlci_peak_rate { no | <kbps> } ]
   [ { -dlci_congestion_management_off | -dlci_congestion_management } ]
   [ -dlci_cir <kbps> ]
   [ { -dlci_ip_outgoing_off | -dlci_ip_outgoing } ]
   [ { -dlci_ipx_outgoing_off | -dlci_ipx_outgoing } ]
   [ { -dlci_inverse_arp_off | -dlci_inverse_arp } ]
   [ { -dlci_provide_arp_off | -dlci-provide_arp } ]
   [ -dlci_bc <kBytes> ]
   [ -dlci_be <kBytes> ]
   [ -dlci_min_access_rate <kbps> ]
   [ -dlci_de_packet_class { no | <No.> } ]
```

Parameters

The initial value items that can be set using frame relay Information and the initial values during initial installation are shown in Table 4-12, “List of Initial Values That Can Be Set Using ISDN Information and Initial Values During Initial Installation,” on page 4-49. For details of each parameter, refer to the configuration definition information in "frame relay information".

Downloaded from www.Manualslib.com manuals search engine

Table 4-10 List of Initial Values that can be set using Frame Relay Information and Initial Values during Initial Installation

Information group name	Information name	Initial value
frame_relay information	Procedure of PVC state report using Frame-Relay protocol	ITU-T Q.933 AnnexA is executed.
	Direction of PVC state report procedure using Frame-Relay protocol	STATUS ENQ is transmitted to wait for STATUS reception.
	Transmission of single PVC non-synchronous state display report using Frame-Relay protocol	Single PVC non-synchronous state display report is not transmitted.
	Delay time from PVC down detection to logical interface down detection using Frame-Relay protocol	0 second
	CLLM reception/monitoring time using Frame-Relay protocol	No CLLM reception is monitored.
	Maximum information field length using Frame-Relay protocol (not including the Q922 header)	1600 bytes
dlci information	Relay designation of packets using Frame-Relay protocol (DLCI)	Send/receive packets are relayed.
	Maximum information field length using Frame-Relay protocol (DLCI) (not including the Q922 header)	1600 bytes
	Limit and maximum value of data transmission rate using Frame-Relay protocol (DLCI)	The transmission rate is not limited.
	Throughput adjustment during detection of frame relay network congestion using Frame-Relay protocol (DLCI)	No throughput adjustment is performed.
	CIR (Certification Information Rate) using Frame-Relay protocol (DLCI)	O kbps
	Setting of IP packet transmission using Frame-Relay protocol (DLCI)	IP packets are transmitted.
	Setting of IPX packet transmission using Frame-Relay protocol (DLCI)	IPX packets are not transmitted (discarded).
	Setting of InverseARP transmission using Frame-Relay protocol (DLCI)	InverseARP is transmitted.
	Setting of ARP transmission using Frame-Relay protocol (DLCI)	ARP is not transmitted.
	BC (certification burst size) using Frame-Relay protocol (DLCI)	0 kBytes
	BE (excess burst size) using Frame-Relay protocol (DLCI)	0 kBytes
	Guarantee value of transmission data rate using Frame-Relay protocol (DLCI)	0 kbps
	DE bit of transmission frame using Frame-Relay protocol (DLCI)	The DE bit is always set to "0".

Downloaded from www.Manualslib.com manuals search engine

4.7.11 ATM Information

Input Format

```
[set]  default
   [ -atm_vpi_vci_range { 1 | 2 | 3 | 4 } ]
   [ -atm_vp_shaping_number { no | 1 | 2 | 4 | 8 | 16 | 32 | 64 } ]
   [ -atm_service_category_pattern {cbr_cbr_ubr_ubr | cbr_cbr_abr_ubr |
   cbr_abr_ubr_ubr | abr_abr_ubr_ubr |
   ubr_ubr_ubr_ubr |
   cbr_cbr_ubr_vbr | cbr_abr_ubr_vbr |
   cbr_ubr_ubr_vbr | abr_ubr_ubr_vbr |
   cbr_cbr_ubr_vbr_exclusive |
   cbr_abr_ubr_vbr_exclusive |
   cbr_ubr_ubr_vbr_exclusive |
   abr_ubr_ubr_vbr_exclusive |
   cbr_ubr_vpshaping_no | ubr |
   gfr_clp_priority | gfr2m |gfr2s}]
   [ -traffic_cbr_priority { 2 | 1 } ]
   [ -traffic_abr_priority { 2 | 1 } ]
   [ -traffic_abr_mcr <Rate> ]
   [ -traffic_abr_icr <Rate> ]
   [ -traffic_ubr_priority { 4 | 3 | 2 | 1 } ]
   [ -traffic_vbr_mbs <Number> ]
   [ -traffic_gfr_threshold_clp1 <Cells> ]
   [ -traffic_gfr_threshold_clp0 <Cells> ]
   [ -traffic_gfr_priority <Cells> ]
   [ -traffic_gfr2_priority4_pcr <Rate> ]
   [ -traffic_gfr2_threshold_priority4_hi <Cells> ]
   [ -traffic_gfr2_threshold_priority4_low <Cells> ]
   [ -traffic_gfr2_threshold_priority3_hi <Cells> ]
   [ -traffic_gfr2_threshold_priority3_low <Cells> ]
   [ -traffic_gfr2_threshold_priority2_hi <Cells> ]
   [ -traffic_gfr2_threshold_priority2_low <Cells> ]
   [ -traffic_gfr2_threshold_priority1_hi <Cells> ]
   [ -traffic_gfr2_threshold_priority1_low <Cells> ]
   [ -traffic_gfr2_priority { 3 | 2 | 1 } ]
   [ { -vp_alarm | -vp_alarm_off } ]
   [ { -vc_enable | -vc_disable } ]
   [ { -vc_inverse_arp | -vc_inverse_arp_off } ]
   [ -vc_mtu <Length> ]
   [ -vc_discard_class { 0 | 1 | 0+1 } ]
   [ -vc_auto_verification { no | <Second> }]
   [ -vc_auto_verification_up_times <Count>]
   [ -vc_auto_verification_down_times <Count>]
   [ -vc_auto_verification_retry_interval <Second>]
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

The initial value items that can be set using ATM Information and the initial values during initial installation are shown in Table 4-11.

Table 4-11 List of Initial Values That Can Be Set Using ARM Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
ATM information	Setting range of VPI and VCI values	3 (VPI=0-63, CVCI=32-511)
	Setting of maximum VP count	64
	Setting of service category pattern	cbr_cbr_ubr_ubr
Traffic information	Setting of cell transmission priority in CBR	2
	Setting of cell transmission priority in ABR	2
	Setting of mcr value in ABR	38kbps
	Setting of icr value in ABR	38kbps
	Setting of cell transmission priority in UBR	4
	Setting of MBS value in VBR	30
	Discard threshold of non-priority packet (CLP1) in GFR	1000cells
	Discard threshold of priority packet (CLP0) in GFR	1500cells
	Setting of cell transmission priority in GFR	3
	pcr value of highest priority packet in GFR2	250kbps
	Priority frame discard threshold of highest priority queue in GFR2	700cells
	Non-priority frame discard threshold of highest priority queue in GFR2	500cells
	Priority frame discard threshold of high priority queue in GFR2	700cells
	Non-priority frame discard threshold of high priority queue in GFR2	500cells
	Priority frame discard threshold of middle priority queue in GFR2	700cells
	Non-priority frame discard threshold of middle priority queue in GFR2	500cells
	Priority frame discard threshold of low priority queue in GFR2	700cells
	Non-priority frame discard threshold of low priority queue in GFR2	500cells
	Setting of cell transmission priority in GFR2	3
VP information	VP warning and loop-back function	A VP warning and loop-back function are used.

Downloaded from www.Manualslib.com manuals search engine

Table 4-11 List of Initial Values That Can Be Set Using ARM Information and Initial Values During Initial Installation (continued)

Information Group Name	Information Name	Initial Value
VC information	Active/non-active state switching of VC	vc_enable (VC active state)
	Switching of mode in which Inverse ARP of an ATM line is used or not used	inverse_arp (Inverse ARP is used.)
	MTU of ATM line	4470 bytes
	Setting of cell loss priority display bit	0 (CLP=0)
	Polling interval in VC state monitoring function using F5-OAM loop-back cell (seconds)	no (The VC state monitoring function does not operate.)
	Number of response reception confirmation times during VC failure recovery in VC state monitoring function using F5-OAM loop-back cell (times)	3 times
	Number of non-response confirmation times during VC failure generation in VC state monitoring function using F5-OAM loop-back cell (times)	5 times
	Request transmission interval during VC failure generation/ recovery in VC state monitoring function using F5-OAM loop-back cell (seconds)	1 second

4.7.12 ISDN Information (Japan Only)

Note: ISDN settings are only valid in Japan.
Software for using the model GR2000-B overseas currently allows the setting of ISDN functions. However, since hardware specifications do not support ISDN, a log message indicating an error is displayed if ISDN configuration definitions are set. In order to avoid this malfunction, do not set ISDN configuration definitions.

Input Format

```
[set]  default
   [ { -isdn_ppp_enable | -isdn_ppp_disable } ]
   [ -isdn_ppp_call_direction { both | originate | answer } ]
   [ -isdn_ppp_min_connect_timer <Second> ]
   [ -isdn_ppp_inactivity_timer <Second> ]
   [ -isdn_ppp_connect_restriction_direction { both | originate} ]
   [ -isdn_ppp_connect_retry_times <Count> ]
   [ -isdn_ppp_connect_retry_interval <Second> ]
   [ -isdn_ppp_max_connect_threshold <Minutes> ]
   [ -isdn_ppp_channel_type { b | h0 | h1 } ]
   [ -isdn_ppp_source_mru <Bytes> ]
   [ -isdn_ppp_echo_trial_times <Count> ]
   [ -isdn_ppp_echo_success_times <Count> ]
   [ { -isdn_ppp_ip_address_negotiation_off |
   -isdn_ppp_ip_address_negotiation } ]
   [ -isdn_ppp_remote_ip_address_mode { assign | check } ]
```


Downloaded from www.Manualslib.com manuals search engine

```
[ { -isdn_ppp_ipx_address_negotiation_off |
-isdn_ppp_ipx_address_negotiation } ]
[ -isdn_ppp_echo_interval <Second> ]
[ -isdn_ppp_authentication_protocol { no | pap | chap | pap_chap } ]
[ -bod_overload_procedure { mp | proprietary } ]
[ -bod_overload_measuring_period { no | <Second>} ]
[ -bod_traffic_watch_type { send | receive | both } ]
[ { -bod_resource_bod | -bod_resource_bod_off } ]
[ -bod_resource_bod_retry_times <Count> ]
[ { -bod_auto_return | -bod_auto_return_off } ]
[ { -bod_provide_phone_number | -bod_provide_phone_number_off } ]
[ -bod_source_mrru <Bytes> ]
[ -bod_add_drop_retry_timer <Second> ]
[ { -backup_auto_return | -backup_auto_return_off } ]
[ { -backup_switch_back_timer <Second> } ]
[ -backup_isdn_call_and_desconnect { quik|on_demand } ]
```

Parameters

The initial value items that can be set using ISDN Information and the initial values during initial installation are shown in Table 4-12. For details of each parameter, refer to the configuration definition information in "ISDN Information".

Table 4-12 List of Initial Values That Can Be Set Using ISDN Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
ISDN information	Use of connection destination	Can be used.
	Outgoing/incoming call type	Used for both outgoing and incoming calls.
	Non-communication monitoring time (just after call setting)	178 seconds
	Non-communication monitoring time (except just after call setting)	60 seconds
	Direction of connection suppression	Both outgoing and incoming calls are suppressed.
	Number of connection retries when a layer 1 failure occurs during ISDN connection	Two times
	Connection retry interval when a layer 1 failure occurs during ISDN connection	6 seconds
	Maximum connection monitoring time	60 minutes
	Type of channel used	Connection of channel B
	Maximum value of MTU length in remote router	4500 bytes
	Number of retries in Echo-RQ frame	7 times
	Minimum number of reception Echo-Reply times for judging "high"-quality link	6 times
	Report of local IP address	The local IP address is not reported.
	Remote IP address mode	A correct IP address is distributed as an IP address distribution request.

Downloaded from www.Manualslib.com manuals search engine

Table 4-12 List of Initial Values That Can Be Set Using ISDN Information and Initial Values During Initial Installation (continued)

Information Group Name	Information Name	Initial Value
ISDN information (continued)	Report of local IPX node number	The local IPX node number is not reported.
	Transmission interval of Echo-RQ frame	3 seconds
	Type of certified protocol	No certified protocol is used.
	Overload connection procedure	Multi-link PPP connection
	Monitoring interval of line usage rate during overloading based on monitoring of line usage rate	The overloading based on the monitoring of a line usage rate is not performed.
	Direction for monitoring of line usage rate	Only the line usage rate during transmission is monitored.
	Operation of resource BOD	Resource BOD is performed.
	Number of ISDN backup connection retries when a failure is detected during connection of ISDN at the backup destination using resource BOD	3 times
	Route change-back procedure of resource BOD	The route is changed back automatically.
	Request of telephone number report to the remote router when a link is added in BAP using an outgoing call	No telephone number is requested.
	Initial value of remote MTU length when using multi-link PPP procedure	4500 bytes
	Request retry interval when the request of link addition and deletion is rejected in BAP	60 seconds
	Backup change-back operation	Automatic change-back
	Surveillance time for manual cut-back.	80 seconds
	ISDN logical port backup switchover and switchback action	Executes call connection prompted by information generation at the time of switchover and executes call disconnection prompted by the detection of no-communication status in information monitoring at the time of switchback.

4.7.13 Tunnel Interface Information

Input Format

```
[set]  default
   [ { -tunnel_optimize_off | -tunnel_optimize } ]
   [-tunnel_mtu <MTU>] [-tunnel_ttl_hoplimit <TTL HopLimit>]
```

Parameters

The initial value items that can be set using tunnel Information and the initial values during initial installation are shown in Figure 1-7.

Downloaded from www.Manualslib.com manuals search engine

Table 4-13 List of Initial Values That Can Be Set Using Tunnel Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
Tunnel information	Optimizing option of tunnel relay performance	off: -tunnel_optimize_off
	Tunnel interface MTU size	1280 octets
	Relay limit count during encapsulation	30

4.7.14 IP Interface Information

Input Format

```
[set]  default
   [ -ip_arp_ageing_time <Minute> ]
   [ -ip_connect_type { point | broad } ]
   [ { -ip_proxy_arp_off | -ip_proxy_arp } ]
   [ -ip_arp_encapsulation { ethernet | probe } ]
   [ -ip_arp_max_send_count { Count } ]
   [ -ip_arp__send_interval { Second } ]
   [ { -ip_source_route_option_forward | -ip_source_route_option_forward_off
   } ]
   [ { -ip_icmp_redirects_off | -ip_icmp_redirects }]
   [ { -ip_icmp6_redirects_off | -ip_icmp6_redirects }]
   [ { -ip_directbroad_forward_off | -ip_directbroad_forward } ]
   [ { -ip_subnetbroad_forward_off | -ip_subnetbroad_forward } ]
   [ { -ip_icmp6_nodeinfo_query | -ip_icmp6_nodeinfo_query_off }]
   [ -ip_rate_limiting <Microsecond> ]
   [ -arp_hardware_type { ethernet | ieee802.3 } ]
   [ -relay_interface_bootp_hops <Hop> ]
```

Parameters

The default value items that can be set using IP Information and the default values during initial installation are shown in Table 4-14. For details of each parameter, refer to the configuration definition information in "GR2000 Configuration Commands, (universal CLI) Vol. 1."

Downloaded from www.Manualslib.com manuals search engine

Table 4-14 List of Default Values That Can Be Set Using IP Information and Default Values During Initial Installation

Information Group Name	Information Name	Initial Value
IP interface information	ARP cache table aging time	30 minutes
	Interface type (Valid only for ATM/ Frame-Relay.)	Broad-type
	Proxy ARP response	No proxy ARP response is made.
	Encapsulation format of ARP request frame (Hardware type)	ethernet
	Maximum number of transmission retries in ARP request frame	4 times
	Transmission retry interval of ARP request frame	2 seconds
	Relay of IP packets with source route option	IP packets with a source router option are relayed.
	ICMP redirect message transmission switch	Transmit
	ICMPv6 redirect message transmission switch	Transmit
	Direct broadcast relay switch	Not relayed.
	Subnet broadcast relay switch	Not relayed.
	Non-response option of ICMPv6 node information query	• The initial value responds. ip_icmp6_nodeinfo_query • To set a non-response option, execute the following. ip_icmp6_nodeinfo_query_off
	rate limiting option (RFC2463)	• The transmission rate of an ICMPv6 error is limited to 1 packet/ <Microsecond> (maximum). • The initial value is enabled(500μs). • To disable this function, set the <Microsecond> value to "0". • The <Microsecond> value can be set up to 1000 in units of 0 to 10.
ARP information	ARP hardware type	Ethernet
DHCP information	Hops threshold value	4

Downloaded from www.Manualslib.com manuals search engine

4.7.15 NAT-PT Information

Input Format

Changing information:

```
[set]  default
     [-natpt_rule_napt_port_range <Start Port> <End Port>]
     [-natpt_rule_protocol [tcp] [udp] [icmp]]
```

Parameters

The default value items that can be set using NAT-PT Information and the default values during initial installation are shown in Table 4-15. For details of each parameter, refer to the configuration definition information in GR2000 Configuration Commands, (universal CLI) Vol. 1.

Table 4-15 List of Default Values That Can Be Set Using NAT-PT Information and Default Values During Initial Installation

Information Group Name	Information Name	Initial Value
IP interface information	ARP cache table aging time	30 minutes
	Interface type (Valid only for ATM/ Frame-Relay.)	Broad-type
	Proxy ARP response	No proxy ARP response is made.
	Encapsulation format of ARP request frame (Hardware type)	ethernet
	Maximum number of transmission retries in ARP request frame	4 times
	Transmission retry interval of ARP request frame	2 seconds
	Relay of IP packets with source route option	IP packets with a source router option are relayed.
	Direct broadcast relay switch	Not relayed.
	Subnet broadcast relay switch	Not relayed.
	Non-response option of ICMPv6 node information query	• The initial value responds. ip_icmp6_nodeinfo_query • To set a non-response option, execute the following. ip_icmp6_nodeinfo_query_off
	rate limiting option (RFC2463)	• The transmission rate of an ICMPv6 error is limited to 1 packet/ <Microsecond> (maximum). • The initial value is enabled(500µs). • To disable this function, set the <Microsecond> value to "0". • The <Microsecond> value can be set up to 1000 in units of 0 to 10.

Downloaded from www.Manualslib.com manuals search engine

Table 4-15 List of Default Values That Can Be Set Using NAT-PT Information and Default Values During Initial Installation

Information Group Name	Information Name	Initial Value
ARP information	ARP hardware type	Ethernet
DHCP information	Hops threshold value	4
NAT-PT information	Port number range of dynamic NAPT-PT conversion rules	<Start Port> 1 <End Port> 65535
	Conversion target protocol of static NAT-PT, dynamic NAPT-PT and static NAPT-PT conversion rules	None (All layer 4 protocol is conversion target)

4.7.16 IPX Information

Input Format

```
[set]  default
   [-ipx_interface_watchdog_spoofing{periodic | proxy | forward } ]
   [ {-ipx_interface_serialization_filtering |
   ipx_interface_serialization_filtering_off }]
   [ { -ipx_interface_diagnostic_packet_forwarding_off |
   ipx_interface_diagnostic_packet_forwarding } ]
   [ { -ipx_interface_non_periodic_rip_send |
   ipx_interface_non_periodic_rip_send_off } ]
   [ { -ipx_interface_non_periodic_sap_send |
   ipx_interface_non_periodic_sap_send_off } ]
   [ -ipx_interface_periodic_rip interface <time>]
   [ -ipx_interface_periodic_sap_interface <time>]
   [ { -ipx_interface_nearest_sap_reply_off_|
   ipx_interface_nearest_sap_reply } ]
   [-ipx_static_sap_socket_number <sockt-number> ]
   [-ipx_static_sap_node_address <MAC-Address> ]
   [ { -ipx_rip_filtering_forward | ipx_rip_filtering_drop }]
   [ { -ipx_rip_filtering_output | ipx_rip_filtering_input }]
   [-ipx_rip_filtering_network <IPX-Address> ]
   [-ipx_rip_filtering_portnetwork <IPX-Address> ]
   [-ipx_sap_filtering_type <Type> ]
   [ { -ipx_sap_filtering_forwayd | ipx_sap_filtering_drop }]
   [ { -ipx_sap_filtering_output | ipx_sap_filtering_input }]
   [-ipx_sap_filtering_server_network <IPX-Address> ]
   [-ipx_sap_filtering_port_network <IPX-Address> ]
   [ { -ipx_filtering_forward | ipx_filtering_drop }]
   [-ipx_filtering_netmask <Mask> ]
   [-ipx_filtering_destination_netmask <Mask> ]
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

The initial value items that can be set using IPX Information and the initial values during initial installation are shown in Figure 1-9. For details of each parameter, refer to the configuration definition information in "Section 2.1, “IPX Objects".

Table 4-16 List of Initial Values That Can Be Set Using IPX Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
IPX interface information	Proxy response function of watchdog packet	A periodic proxy response is made. (periodic)
	Filter function during serialization packet reception	Discarded. (ipx_interface_serialization_filtering)
	Filter function during diagnostic packet reception	Discarded. (ipx_interface_diagnostic_packet_forwarding_off)
	Non-periodic RIP response/ transmission switch	Replied and transmitted. (ipx_interface_nonperiodic_rip_send)
	Non-periodic SAP response/ transmission switch	Replied and transmitted. (ipx_interface_nonperiodic_sap_send)
	Periodic RIP transmission interval	1 (minute)
	Periodic SAP transmission interval	1 (minute)
	Nearest SAP response switch	No response is made. (ipx_interface_nearest_sap_reply_off)
	Socket number of static SAP	0x0451
	Server node address of static SAP	00:00:00:00:00:01
	Operation designation of RIP filter	Relayed. (ipx_rip_filtering_forward)
	Mode designation of RIP filter	Output designation (ipx_rip_filtering_output)
	Network designation of RIP filter	Total designation (0xffffffff)
	Interface of RIP filter	Total destination (0xffffffff)
	Type designation of SAP filter	0xffff
	Operation designation of SAP filter	Relayed. (ipx_rip_filtering_forward)
	Mode designation of SAP filter	Output designation (ipx_rip_filtering_output)
	Network designation of RIP filter	Total designation (0xffffffff)
	Interface of RIP filter	Total designation (0xffffffff)
	Operation designation of ipx filter	Relayed. (ipx_filtering_forward)
	net-mask designation of ipx filter	0x00000000
	Destination net-mask designation of ipx filter	0x00000000

Downloaded from www.Manualslib.com manuals search engine

4.7.17 Bridge information

Input Format

```
[set]  default
   [-bridge_interface_action {no | spt | yes }]
   [-bridge_interface_cost_ <Number> ]
   [-bridge_interface_priority <Number> ]
   [ { -bridge_interface_enable | bridge_interface_disable }]
   [ { -bridge_interface_translation off |
   _bridge_interface_translation } ]
   [-bridge_extended_filtering_action  { no | yes } ]
   [-bridge_extended_filtering_type  { off | da | dasp | ssap | cti |
   oui | pid | type | user }]
   [-bridge_extended_filtering_value <Number> ]
   [-bridge_extended_filtering_mask <Number> ]
   [-bridge_extended_filtering_offset <Number> ]
```

Parameters

The initial value items that can be set using bridge Information and the initial values during initial installation are shown in Table 4-17. For details of each parameter, refer to the configuration definition information in "Section 2.2, “Bridge Objects".

Table 4-17 List of Initial Values That Can Be Set Using IPX Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
Bridge information	Designation of bridge interface mode	Operation is disabled. (no)
	spt path cost	10
	spt priority	128
	Bridge interface operation	Possible (bridge_interface_enable)
	FDDI translation	Not translated. (bridge_interface_translation_off)
	Extended filtering operation	Operates in drop. (no)
	Designation of extended filtering item	No information is provided. (off)
	Extended filtering data value	0x000000000000
	Extended filtering mask value	0x000000000000
	Extended filtering offset value	0

Downloaded from www.Manualslib.com manuals search engine

4.7.18 QoS Information

Input Format

```
[set]  default
   [ { -qos_queue_list_priority
   | -qos_queue_list_bandwidth
   | -qos_queue_list_round_robin
   | qos_queue_list_equal_bandwidth
   | -qos_queue_list_bandwidth_kbps } ]
   [ -qos_queue_list_que_number <Number> ]
   [ { -qos_queue_list_max_queue_number_4(*1)ÅyROUTE-OS6BÅz
   | -qos_queue_list_max_queue_number_8
   | -qos_queue_list_max_queue_number_16
   | -qos_queue_list_max_queue_number_32
   | -qos_queue_list_max_queue_number_64(*1)[ROUTE-OS6B]
   | -qos_queue_list_max_queue_number_250
   | -qos_queue_list_max_queue_number_1000 }]
   [ -queue <Queue No.>,<Queue No.> - < Queue No.>,Åc<min rate (kbps)> ]
   [ -qos_discard_mode <Number> ]
   [ { -qos_ip_list_ip_pair | -qos_ip_list_ip_pair_off } ]
   [ { -qos_ip_list_port_pair | -qos_ip_list_port_pair_off } ]
   [ { -qos_ip_list_pair_synchronized_off | -qos_ip_list_pair_synchronized }
   ]
   [ { -qos_ip_list_max_priority_class_8
   | -qos_ip_list_max_priority_class_16
   | -qos_ip_list_max_priority_class_32 } ]
   [ -qos_ip_list_priority_class <Number> ]
   [ -qos_ip_list_discard_class <Number> ]
   [ -qos_ipx_discard_class <Number> ]
   [ -qos_ipx_priority_class <Number> ]
   [ -qos_bridge_discard_class <Number> ]
   [ -qos_bridge_priority_class <Number> ]
   [ -qos_hdlc_discard_class <Number> ]
   [ -qos_hdlc_priority_class <Number> ]
```

(1*) For the maximum queue number, refer to the “*qos-gueue-list* (QoS queue attribute)."

Parameters

The initial value items that can be set using QoS Information and the initial values during initial installation are shown in Table 4-18. For details of each parameter, refer to the configuration definition information in "Section 1.2, “Quality of Service (QoS) Objects".

Downloaded from www.Manualslib.com manuals search engine

Table 4-18 List of Initial Values That Can Be Set Using QoS Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
QoS information	Queue mode of queue list	Output priority control
	Number of queues in which the band is equally assigned when the queue mode of a queue list is a minimum equal band guarantee	24
	Maximum number of queues when the queue mode of a queue list is a minimum band guarantee (specified in kbit/s)	8
	Minimum band when the queue mode of a queue list is a minimum band guarantee (specified in kbit/s)	0
	Discard mode	Discard mode 3
	Check of source and destination IP addresses	The source and destination IP addresses are checked for replacement without replacement.
	Check of source and destination upper protocol port numbers	The source and destination upper protocol port numbers are checked for replacement without replacement.
	Sequential check of IP address and upper protocol port number	The source and destination IP addresses, and source and destination upper protocol port numbers are simultaneously checked without replacement, respectively.
	Designation of maximum output priority class	8
	Designation of output priority class (for IP)	Class 4
	Designation of queuing priority class (for IP)	Class 4
	Designation of output priority class (for IPX)	Class 4
	Designation of queuing priority class (for IPX)	Class 4
	Designation of output priority class (for bridge)	Class 4
	Designation of queuing priority class (for bridge)	Class 4
	Designation of output priority class (for hdlc)	Class 4
	Designation of queuing priority class (for hdlc)	Class 4

Downloaded from www.Manualslib.com manuals search engine

4.7.19 Filter Information

Input Format

```
[set]  default
     [ { -filter_forward | -filter_drop } ]
     [ { -filter_ack_check_off | -filter_ack_check } ]
     [ { -filter_syn_check_off | -filter_syn_check } ]
     [ { -filter_pair_synchronized_off | -filter_pair_synchronized } ]
     [ { -filter_ip_pair | -filter_ip_pair_off } ]
     [ { -filter_port_pair | -filter_port_pair_off } ]
```

Parameters

The initial value items that can be set using filter Information and the initial values during initial installation are shown in Table 4-19. For details of each parameter, refer to 1.1.10 to 1.1.13 in this guide for filter information.

Table 4-19 List of Initial Values That Can Be Set Using Filter Information and Initial Values During Initial Installation

Information Group Name	Information Name	Initial Value
Filter information	Operation when filter information coincides with filter conditions	Not relayed.
	Designation of TCP one-way communication permission (ACK flag)	The packet whose ACK flag is 1 is not treated for filtering.
	Designation of virtual circuit establishment permission (SYN flag)	The packet whose SYN flag is 1 is not treated for filtering.
	Sequential check of IP address and upper protocol port number	The source and destination IP addresses, and source and destination upper protocol port numbers are checked without replacement.
	Check of source and destination IP addresses	The source and destination IP addresses are checked for replacement without replacement.
	Check of source and destination upper protocol port numbers	The source and destination upper protocol port numbers are checked for replacement without replacement.

Downloaded from www.Manualslib.com manuals search engine

4.7.20 router-default

Function

Displays the initial default values for the router configuration with the show subcommand.

Input Format

```
show router-default
```

Parameters

None

Example

```
(config)# show router-default
abbrev.
(config)#
```

Related Configuration Object

router-default

Precautions

None

Downloaded from www.Manualslib.com manuals search engine

Chapter 5
Configuration Error Messages

This chapter describes error messages displayed when you enter configuration commands.

Downloaded from www.Manualslib.com manuals search engine

5.1 Common

Table 5-1 Configuration Error Messages

Message	Contents
Can not execute *config* command, please try again.	Communication error occurred between processes.Wait for recovery, then execute again.
Command incomplete because processing configuration deletion exceeded time limit.To complete deletion, please try same command again.	Because processing deletion of configuration is taking too much time, command is interrupted.Execute same command again. For example, if this message is displayed during the deletion of line information, the IP information and line information may not have been deleted even if the IP routing protocol has been removed.
Configuration file is closed.	Current or spare configuration file closed.After opening current or spare configuration file, execute configuration command again.
illegal option -- <Option>	Illegal option entered. Correct the option.
Interface name not found.	Specified interface name not found. Specify a correct interface name.
Invalid subcommand.	Subcommand invalid. Enter a correct subcommand.
<item> is not in range <value1> to <value2>.	The value is out of range. Set the in-range value. <item>Parameter name, <value1> Minimum value, <value2>Maximum value
Logical inconsistency occurred.	An internal program complication has occurred in editing and processing the configuration defining information. Collect the following log information and deliver it to the maintenance person. The maintenance person will send the log information to the assisting department. [Procedure to collect log information] 1. Set the terminal so that the screen logs can be collected. 2. Execute the following commands. (1) *cat/var/tmp/gen/genTrace_config* (2) *cat/var/tmp/gen/genTrace_configManager* (3) */usr/local/diag/configShowBinary* 3. Finish collecting the screen logs.
Maximum number of entries are already defined.	Attempt made to add entries exceeding the limit. Delete unnecessary entries, then add an entry.
No enough parameters.	The parameters are insufficient. Specify the necessary parameters.
No such delete index	Because the entered value is illegal, configuration information cannot be deleted. Enter a correct value.
No such insert index	Because the entered value is illegal, configuration information cannot be inserted. Enter a correct value.
No such <object>	The configuration defining information for the name designated in the <object> is not available. Designate the name of the defining information being set.
Now another user configured, please try again.	Another user is currently changing the configuration. Wait for access, then execute again.
Now configuration data is changing, please try again.	Configuration information being changed. Wait for the change, then execute again.
Now configuration file is locked, please try again.	The operating configuration defining information cannot be edited because another user is referencing it using the command. If "more" is displayed in the operation command that indicates the interface name, finish the "more" display, and execute the command again. If “more” is not displayed, execute it again after a while.
Operation not permitted	Because operation configuration information written in memory is being edited, operation is not permitted.
option requires an argument -- <Option>	Option entry insufficient. Correct the option.

Downloaded from www.Manualslib.com manuals search engine

Table 5-1 Configuration Error Messages (continued)

<Option> out of range	The option entered exceeds the maximum value. Recheck the option.
<Option> too long	The number of sentences in the option exceeds the maximum value. Recheck the option.
The total of <item> exceeded <value>.	The total of <item> exceeded <value>. Set the value in the range. <item>Parameter name, <value 1-1>Maximum value
This router is operated using the configuration data created in "CLI(CLItype1)" mode.	This router operates with configuration information produced in the CLI type 1 mode.
This router is operated using the configuration data created in "Universal CLI(CLItype2)" mode.	This router operates with configuration information produced in the CLI type 2 mode.

5.2 Router Control Information

Table 5-2 Router Control Information Error Messages

Message	Contents
Can not disable HTTP access because a user is logged in from a browser.	Since the user has performed log-in by using a browser, log-in using the HTTP protocol cannot be prohibited. To prohibit log-in using the HTTP protocol, perform log-out from this device.
Invalid local IP address.	Local IP address value invalid. Enter a correct local IP address.
Invalid remote access IP address.	Remote access IP address value invalid. Enter a correct P address of remote access terminal.
Relations between local address and destination ip address in ip configuration are inconsistent.	Relations between relations between local address and IP address or destination IP address in IP configuration are inconsistent. Set local address different from IP address or destination IP address in IP (No VPN definition) configuration.
Remote access IP address not specified.	IP address of remote access terminal has not been specified. Specify IP address of remote access terminal.

Downloaded from www.Manualslib.com manuals search engine

5.3 Network Interface

Table 5-3 Network Interface Error Messages

Message	Contents
AC name is longer than 32 characters.	The designated AC name is greater than 32 characters. Designate the AC name with 32 or fewer characters.
Atm not specified.	ATM is not set. Set a ATM.
Aux is not supported.	Can not set a AUX. AUX is not supported.
Bod in ppp configuration not specified.	Bod in ppp configuration not specified. When ISND PPP is grouped with PPP, set Bod to PPP in group.
Bod with group configuration not specified.	Bod with grouped Isdn PPP configuration not specified. When ISDN PPP is grouped with PPP, set the same Bod with PPP within the group to PPP.
Can not be set because there are parameters other than the interface name in the IP configuration.	Since there are parameters other than interface name in IP definitions, it is not possible to set EoMPLS L2 transports.
Can not bind interface to Frame Relay since the interface has already been bound to PPP.	Attempt to built frame relay in interface which has ready been set PPP. Delete Frame Relay information first, then set PPP.
Can not bind interface to PPPoE since the interface has already been bound to VLAN	Attempt made to built PPPoE in interface which has ready been set VLAN. Delete VLAN information first, then set PPPoE.
Can not bind interface to PPP since the interface has already been bound to Frame Relay.	Attempt made to built PPP in interface which has ready been set frame relay. Delete Frame Relay information first, then set PPP.
Can not bind interface to VLAN since the interface has already been bound to PPPOE	Attempt made to built VLAN in interface which has ready been set PPPoE. Delete PPPoE information first, then set VLAN.
Can not delete line with PPPoE configuration	PPPoE information is present. Delete the PPPoE information, and then delete the line.
Can not delete PPPoE configuration with IP or group configuration	Attempting to delete the IP "IP information" or PPPoE of the grouped interface. Delete the IP "IP information" and then delete the PPPoE.
Can not change <name>.	Can not change <name>. To change name, delete the name first and then set the specified name.
Can not change line group name.	Line group name has already set in line group of different RP number. Set the line on the same RP.
Can not change line type.	The line type cannot be changed. To change, delete line type and add it again.
Can not change subline no.	Can not change subline no. To change name, delete the name first and then set the specified subline no.
Can not delete ATM configuration with vp configuration.	VP information present. Delete VP; delete ATM information.
Can not delete bod configuration with isdn_ppp configuration.	ISDN PPP information present. Delete ISDN PPP; delete Bod information.
Can not delete bod configuration with ppp configuration.	PPP information present. Delete PPP; delete Bod information.
Can not delete DLCI configuration referred by ARP configuration.	IP ARP information present. Delete IP ARP; delete DLCI information.
Can not delete DLCI configuration referred by ipx_arp configuration.	IPX ARP information present. Delete IPX ARP; delete DLCI information.
Can not delete DLCI configuration referred by QoS interface configuration.	QoS interface present. Delete QoS interface; delete DLCI.
Can not delete DLCI configuration with IP or group configuration.	Attempt made to delete DLCI of the interface with IP information or group. Delete IP information or group; delete the DLCI information.
Can not delete Frame Relay configuration referred by QoS interface configuration.	QoS interface present. Delete QoS interface; delete frame relay.
Can not delete Frame Relay configuration with dlci configuration.	DLCI information present. Delete QoS interface; delete frame relay.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Can not delete Frame Relay configuration with IP configuration.	Attempt made to delete an frame relay of interface in IP information or group. Delete IP information or group; delete the frame relay.
Can not delete group configuration referred by QoS IP configuration.	Attempt made to delete interface specified by QoS IP configuration. Delete the target interface specification of QoS IP; delete the interface.
Can not delete group configuration referred by QoS bridge configuration.	Attempt made to delete interface specified by QoS bridge configuration. Delete the target interface specification of QoS bridge; delete the group.
Can not delete group configuration referred by QoS hdlc passthrough configuration.	Attempt made to delete an group specified by QoS hdlc passthrough configuration. Delete an group specified by QoS hdlc passthrough configuration first.
Can not delete group configuration referred by bridge extended filtering configuration.	Attempt made to delete group configuration specified by bridge extended filtering configuration. Delete the target interface specification of bridge extended filtering configuration; delete the group.
Can not delete group configuration referred by bridge filtering database configuration.	Attempt made to delete group specified by bridge filtering database configuration. Delete the target interface specification of filtering database; delete the group.
Can not delete group configuration referred by filter interface configuration.	You are about to remove the interface designated for the IP filtering interface. Before removing the interface, disable the designation of the IP filtering interface.
Can not delete group configuration referred by filter list configuration.	You are about to remove the interface designated in the IP filtering list. Before removing the interface, disable the designation of the interface in the IP filtering list.
Can not delete group configuration referred by QoS IPX configuration.	You are about to remove the interface designated by QoS IPX. Before removing the interface, remove the interface for QoS IPX.
Can not delete group configuration referred by IPX filtering configuration.	You are about to remove the interface designated for IPX filtering. Before removing the interface, disable the designation of the interface for IPX filtering.
Can not delete group configuration with bridge interface.	You are about to remove the group complete with bridge interface settings. Before removing the group, remove the bridge interface.
Can not delete group configuration with IP configuration.	You are about to remove the interface complete with IP settings. Before removing the interface, delete the IP settings.
Can not delete group configuration with IPX interface.	You are about to remove the group complete with IPX interface settings. Before removing the group, delete the IPX interface settings.
Can not delete group dlci with dlci-group replace.	You are about to remove the DLCI set in "replace" of the dlci-group. Before removing the group or its DLCI, delete "replace" of the dlci-group.
Can not delete group dlci with dlci-group.	You are about to remove DLCI set in the dlci-group. Before removing the group or its DLCI, delete DLCI in the dlci-group.
Can not delete group vc with vc-group.	You are about to remove VC set in the vc-group. Before removing the group or its VC, delete VC in the vc-group.
Can not delete isdn_ppp configuration with arp configuration.	Can not delete isdn_ppp configuration with ARP configuration. Delete the ARP information first and then delete the Isdn Ppp information.
Can not delete isdn_ppp configuration with IP or group configuration.	Can not delete isdn_ppp configuration with IP or group configuration. Delete the IP information or group first and then delete the Ppp information.
Can not delete isdn_ppp configuration with ipx_arp configuration.	Can not delete isdn_ppp configuration with IPX_ARP configuration. Delete the IPX ARP information first and then delete the Isdn Ppp information.
Can not delete isdn_ppp configuration with QoS interface configuration.	Can not delete isdn_ppp configuration with QoS interface configuration. Delete the QoS interface information first and then delete the Isdn Ppp information.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Can not delete line referred by QoS interface configuration.	QoS interface information exists. Delete QoS interface information; delete the line.
Can not delete line with ARP configuration.	IP ARP information exists. Delete IP ARP information and delete the line.
Can not delete line with ATM configuration.	IP ATM information exists. Delete IP ATM information and delete the line.
Can not delete line with dch line of line group configuration.	Can not delete line with dch line of line group configuration. Delete first the Dch line of entry other than Line Group.
Can not delete line with Frame Relay configuration.	Frame Relay information exists. Delete Frame Relay information; delete the line.
Can not delete line with IP or group configuration.	Attempt made to delete a grouped line or a line where IP information exists. Delete IP information or group and delete the line.
Can not delete line with ISDN_PPP configuration.	Can not delete line with ISDN_PPP configuration. Delete the Isdn Ppp information first and then delete the line.
Can not delete line with LINE GROUP configuration.	Can not delete line with LINE GROUP configuration. Delete the Line Group information first and then delete the line.
Can not delete line with line (aps protection) configuration.	Line (aps protection) information exists. Delete line (aps protection) information and delete the line.
Can not delete line with POOL configuration.	ISDN POOL information exists. Delete the Isdn Pool information first and then delete the line.
Can not delete line with PPP configuration.	PPP information exists. Delete PPP information; delete the line.
Can not delete line with RMON history control configuration.	Attempt made to delete a line where RMON history control information is set. Correct line item in the RMON history control and delete the line.
Can not delete line with subline configuration.	Subline information exists. Delete subline information; delete the line.
Can not delete line with timeslot configuration.	Timeslot information exists. Delete timeslot information; delete the line.
Can not delete line_group configuration with pool configuration.	ISDN POOL information exists. Delete ISDN POOL information first and then delete the Line Group information.
Can not delete pool configuration with isdn_ppp configuration.	Can not delete pool configuration with isdn_ppp configuration. Delete the Isdn Ppp information first and then delete the Isdn Pool information.
Can not delete PPP configuration referred by QoS interface configuration.	QoS interface information present.Delete QoS interface information; delete PPP information.
Can not delete PPP configuration with IP or group configuration.	Attempt made to delete PPP configuration with IP or group configuration. Delete IP information or group; delete PP information.
Can not delete subline configuration with timeslot configuration.	Timeslot information present. Delete Timeslot information; delete subline information.
Can not delete timeslot configuration with Frame Relay configuration.	Frame Relay information present. Delete Frame Relay information; delete timeslot information.
Can not delete timeslot configuration with PPP configuration.	PPP information present. Delete PPP information; delete timeslot information.
Can not delete traffic configuration referred by vc configuration.	VC information present. Delete VC information; delete traffic information.
Can not delete TUNNEL configuration with IP or group configuration.	You are about to remove the TUNNEL of IP information or a grouped interface. Before removing the TUNNEL information, delete the IP information or the group.
Can not delete vc configuration with arp configuration.	ARP information present. Delete ARP information; delete VC information.
Can not delete vc configuration with IP or group configuration.	You are about to remove the VC of IP information or a grouped interface. Before removing the VC information, delete the IP information or the group.
Can not delete vc configuration with ipx_arp configuration.	IPX ARP information present. Delete IPX ARP information; delete VC information.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Can not delete vc configuration with QoS interface configuration.	Qos interface information present. Delete Qos interface information; delete VC information.
Can not delete vp configuration with vc configuration.	VC information present. Delete VC information; delete VP information.
Can not set adtf.	Can not set adtf. Confirm the traffic type.
Can not set bod.	BOD is set on the POS line. You are not permitted to set BOD for the POS line.
Can not set bri topology on priisdn.	The interface type cannot be set to priisdn.
Can not set call reference length on priisdn.	The call number length cannot be set to priisdn.
Can not set cdf.	Can not set cdf. Confirm the traffic type.
Can not set dch line.	Can not set dch line. When own telephone number is undefined on Priisdn line, Dch line cannot be set.
Can not set frtt.	Can not set frtt. Confirm the traffic type.
Can not set icr.	Can not set icr. Confirm the traffic type.
Can not set line.	Can not set line. To set an APS line, set an OC line in the same NIF.
Can not set mbs.	Can not set mbs. Confirm the traffic type.
Can not set mcr.	Can not set mcr. Confirm the traffic type.
Can not set multiple timeslot.	Multiple timeslots cannot be set. Multiple timeslots are not supported.
Can not set pcr.	Can not set pcr. Confirm the traffic type.
Can not set priority.	Can not set priority. Confirm the traffic type.
Can not set priority3 pcr.	Can not set priority3 pcr. Confirm the traffic type.
Can not set rdf.	Can not set rdf. Confirm the traffic type.
Can not set rif.	Can not set rif. Confirm the traffic type.
Can not set scr.	Can not set scr. Confirm the traffic type.
Can not set tbe.	Can not set tbe. Confirm the traffic type.
Can not set threshold clp0.	Can not set threshold clp0. Confirm the traffic type.
Can not set threshold clp1.	Can not set threshold clp1. Confirm the traffic type.
Can not set threshold priority1 hi.	Can not set threshold priority1 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority1 low.	Can not set threshold priority1 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority2 hi.	Can not set threshold priority2 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority2 low.	Can not set threshold priority2 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority3 hi.	Can not set threshold priority3 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority3 low.	Can not set threshold priority3 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority4 hi.	Can not set threshold priority4 hi. "Confirm the traffic type" cannot be set.
Can not set threshold priority4 low.	Can not set priority3 pcr. "Confirm the traffic type" cannot be set.
Can not set timeslot.	Can not set timeslot. Recheck the line type to set the time slot.
Can not set tunnel interface.	Can not set tunnel interface. Confirm the interface setting number per RP. If an RP set with 256 interfaces is present, the tunnel interface cannot be set.Change the configuration definition so that the number of interfaces set in the applicable RP is less than 255 and then re-actuate the device.
Can not set vlan	A VLAN line cannot be set. Set it to RP and NIF compatible with Tag-VLAN when setting a VLAN line.
Can not support vlan.	Not compatible with a VLAN line. Use RP and NIF compatible with Tag-VLAN when using a VLAN line.
Connect type is not point.	Connect type is not point. Specify point to the IP type.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Dch line not specified.	Dch line not specified. When own telephone number is undefined on Priisdn line, set Dch line.
Dlci not specified.	A DLCI value has not been specified. Specify a DLCI value.
Duplicate dlci.	The same DLCI values are used in the line. Make each DLCI value in the line unique.
Duplicate IP address.	The same IP address is set. The combination of a local address and a remote address is set in another entry.
Duplicate subline number.	The same subline number is used. Make each timeslot number in the same line unique.
Duplicate timeslot.	The same timeslot number is used. Make each timeslot number in the same line unique.
Duplicate vc.	The same VCI in VP is set. Set the unique value to all of the VCI in VP.
Duplicate vpi.	The same VPI in ATM is set. Set the unique value to all of the VPI in ATM.
Echo success times is greater than echo trial times.	The reference for Link Quality OK exceeds the number of link quality tests. Set the reference for Link Quality OK below the number of link quality tests.
Invalid backup interface name.	Invalid backup interface name. Specify the different interface name to backup source and backup destination. Or, specify the interface not specified by other entry to backup destination interface name.
Invalid bod.	Invalid bod. When Isdn Ppp is grouped with Ppp, set the same Bod with other entry within the group to Ppp.
Invalid bod.	Invalid bod. When Isdn Ppp is grouped, set the same Bod with other entry within the group to Ppp.
Invalid dch line.	Invalid dch line. Set the line without Dch line in line group.
Invalid interface name.	Invalid interface name. Specify the interface not specified by other entry to backup destination interface name.
Invalid line number.	Specified line number not present in NIF. Specify a line number for NIF.
Invalid line type.	Invalid line type. Different line types are set within the same NIF.
Invalid local IP address.	Local IP address value invalid. Enter a correct local IP address.
Invalid name <name>.	Can not specify entered name of configuration information. For subline: Set line name whose line type is ce3 For Timeslot: Specify either line name whose line type is bri, pri, j2, t1, e1, or subline name. For PPP: Specify either line name whose line type is serial, oc3pos, oc12pos, oc48pos, t3, e3, or name of timeslot. For Frame Relay: Specify either line name whose line type is serial or name of timeslot. For DLCI: Specify name set in frame relay. For DLCI group: Specify name set in DLCI. For Line Group: Line type is ISDN POOL on briisdn and Priisdn. Specify a line on the same RP that is not set on the ISDN PPP. For ISDN POOL: Line type is ISDN POOL on briisdn and Priisdn. Specify a line on the same RP that is not set on the ISDN PPP or the name of a Line Group on the same RP. For ISDN PPP: Line type is ISDN POOL on briisdn and Priisdn. Specify a line on the same RP that is not set on the ISDN POOL or the name of an ISDN POOL on the same RP. For ATM, VP, VC: Specify the line name whose line type is oc3atm, oc12atm, 25atm. For VC group: Specify VC on the same line. Specify vc on the same line. For group: Specify DLCI, VC, PPP, ISDN PPP name on the RP already defined.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Invalid phone number.	Invalid phone number. Set own telephone number in the line that set own telephone number to the same.
Invalid physical interface type.	The interface type of the backup server is illegal. The Ethernet or frame relay may not be designated.
Invalid remote IP address.	The remote IP address is illegal. If the local IP address is IPV4, set the remote IP address to IPV4. Or, if the local IP address is IPV6, set the remote IP address to IPV6.
Invalid remote IP address.	The remote IP address is illegal. Set the correct remote IP address. Or use different IP addresses for the local and remote servers. Or, the IPV6 local address and the IPV6 remote address are not in the same scope.
Invalid timeslot number.	In the J2 timeslot: Although channel width is 24 or less, it exceeds the range of 96 timeslots and quartered 24 timeslots. --> Although the channel width exceeds 24, it is not 1, 25, or 49. Specify the value so the timeslot number and timeslot specified in channel width are within the 24 timeslots defined by quartering 96 timeslots. --> Specify 1, 25, or 49 in the timeslot number.
Invalid traffic.	Traffic invalid. Set a correct traffic.
IP address configuration not specified.	IP address configuration not specified. Set IP address.
IP configuration not specified.	IP routing has not been specified. Specify IP routing.
Line already defined.	A line is already defined. Define the line in another line number.
LINE No. out of range.	Specified line number exceeds maximum value. Check the line number.
Links not specified.	Links not specified. Set overload link count.
Max packet size is greater than max packet size (Frame Relay).	Field maximum value is greater than the Frame Relay field maximum value. Specify the value so the field maximum value is no greater than the Frame Relay maximum value.
Max packet size is less than dlci max packet size(dlci).	Field maximum value is less than some DLCI field maximum values. Correct DLCI field maximum values so they are more than all DLCI field maximum values of this line.
Maximum number of DLCI configurations are already defined.	No more DLCI configurations can be defined. Check the network configuration.
Maximum number of ethernet line are already defined.	No more Ethernet lines can be added. Check the network configuration.
Maximum number of Frame Relay configurations are already defined.	No more Frame Relay configurations can be set. Check the network configurations.
Maximum number of isdn_ppp configurations are already defined.	No more isdn_ppp configurations can be set. Check the network configuration.
Maximum number of NIF are already defined.	No line settings are possible. Recheck the number of lines per RP.
Maximum number of PPP configurations are already defined.	No more PPP configurations can be set. Check the network configurations.
Maximum number of pppoe configurations are already defined.	No more PPPoE configurations can be set. Check the network configurations.
Maximum number of traffic are already defined.	256 types of traffic per line are already set. Check the network configuration.
Maximum number of traffic ubr are already defined.	Maximum number of traffic ubr are already defined. Check the network configuration.
Maximum number of TUNNEL configurations are already defined.	No more TUNNEL configurations can be set. Check the network configurations.
Maximum number of vc are already defined.	2048 vc per line are already defined. Check the network configuration.
Maximum number of vc configurations are already defined.	Maximum number of vc configurations are already defined. Check the network configuration.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Mcr not specified.	MCR not specified. Set MCR.
Minimum rate is greater than server rate2.	The minimum transmission throughput during control under heavy congestion exceeds the minimum ratio of 2 of transmission throughput to the net under changing heavy congestion. Adjust settings so as to reduce the minimum throughput during control to below the minimum ratio of 2 of transmission throughput to the net under changing heavy congestion
Monitored events counter is less than error threshold.	Link quality monitored event interval is less than the error threshold of link quality. Set the value so the link quality monitored event interval is no less than the error threshold of link quality.
NIF board is not mounted.	Type of the mounted device is not found. Mount device.
NIF board type is mismatched.	Specified type is different from type of mounted device. Specify type of mounted device.
NIF No. out of range.	Specified NIF number exceeds maximum value. Check the NIF number.
No pvc detection id less than value multiplied by t391 dte timer and error threshold.	The PVC unavailability message receive count is less than the value multiplied by the status inquiry request message send interval and the error frequency used for detecting falling. Set the value so the PVC unavailability message receive count is no less than the value multiplied by the status inquiry request message send interval and the error frequency used for detecting falling.
No such ATM configuration.	No such ATM configuration. Confirm the specified name.
No such name <name>.	Specified configuration information name not found. Specify existing definition information name.
No such set index.	An entry cannot be set on specified entry number. Use entry number not exceeding the set number of entries. To add entries, use the number of set entries +1 for entry value.
No such vp configuration.	No such vp configuration. Confirm the specified name or vp value.
Pcr not specified.	Pcr not specified. Set PCR.
Phone number not specified.	Own phone number not specified. Set the own telephone number to Dch line.
Relations between aps and line (aps protection) are inconsistent.	Relations between aps type and line (aps protection) are inconsistent. If the APS lines are set in the same NIF, set the APS operation switch to ON.
Relations between aps_protocol, revertive and directional are inconsistent.	Relations between aps_protocol, revertive and directional are inconsistent. Set the correct value.
Relations between authentication protocol and phone number1 are inconsistent.	Relations between authentication protocol and phone number1 are inconsistent. When authentication protocol is no, set peer's phone number and subaddress 1.
Relations between authentication protocol and user name and password are inconsistent.	Relations between authentication protocol and user name and password are inconsistent. When authentication protocol is other than no, set own user ID and own password.
Relations between authentication protocol and user name and password are inconsistent.	Relations between authentication protocol and user name and password are inconsistent. When authentication protocol is other than no, set own user ID and own password.
Relations between cir and bc are inconsistent.	Authentication burst size is greater than transmission throughput/ 8x40. Specify the authentication burst size not exceeding transmission throughput/8x40.
Relations between echo trial times and echo success times are inconsistent.	Relations between echo trial times and echo success times are inconsistent. Set standard value of link quality OK to the trial count of link quality judge or less.
Relations between inverse arp and local management (frame relay) are inconsistent.	Although the PVC status check protocol is no, the InARP address solving execution is on. Turn off the InARP address solving execution switch.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Relations between local management and inverse arp(dlci).	Although the DLCI InARP address solving execution switch is on, PVC status check protocol is "no."Set the PVC status check protocol to q933.
Relations between mcr and icr are inconsistent.	Relations between mcr and icr are inconsistent. Set to MCR =< ICR.
Relations between mcr and pcr are inconsistent.	Relations between mcr and pcr are inconsistent. Set to MCR =< PCR.
Relations between mcr, pcr and priority4 pcr are inconsistent.	Relations between mcr, pcr and priority4 pcr are inconsistent. Set the correct value.
Relations between overload link add threshold and overload link drop threshold are inconsistent.	Relations between overload link add threshold and overload link drop threshold are inconsistent. Set overload start line usage ratio larger than overload stop line usage ratio.
Relations between overload measuring period and overload link add threshold and overload link drop threshold are inconsistent.	Relations between overload measuring period and overload link add threshold and overload link drop threshold are inconsistent. When overload measurement interval is other than no, set overload start line usage ratio and overload stop line usage ratio.
Relations between pcr and icr are inconsistent.	Relations between pcr and icr are inconsistent. Set to ICR =< PCR.
Relations between pcr and mcr are inconsistent.	Relations between pcr and mcr are inconsistent. Set to MCR =< PCR.
Relations between phone number and interface id are inconsistent.	The relationship between the local phone number, sub-address and the interface ID. Recheck the value to be set.
Relations between priority4 pcr and pcr are inconsistent.	Relations between priority4 pcr and pcr are inconsistent. Set the correct value.
Relations between scr and pcr are inconsistent.	Relations between scr and pcr are inconsistent. Set to SCR =< PCR.
Relations between service category pattern, traffic mcr and traffic pcr are inconsistent.	Relations between service category pattern, traffic mcr and traffic pcr are inconsistent. Set the correct value.
Relations between service category pattern and traffic pcr are inconsistent.	Relations between service category pattern and traffic pcr are inconsistent. Set the correct value.
Relations between service category pattern and traffic type are inconsistent.	Relations between service category pattern and traffic are inconsistent. Specify the service category pattern traffic type appropriate for the traffic type.
Relations between service category pattern and vp shaping number are inconsistent.	Relations between service category pattern and vp shaping number are inconsistent. Specify the maximum VP count of VP shaper appropriate for the service category pattern.
Relations between share and vp alarm are inconsistent.	Relations between share of DLCI/VC group and vp alarm are inconsistent. Set to share = VP alarm.
Relations between threshold clp1 and threshold clp0 are inconsistent.	Relations between threshold clp1 and threshold clp0 are inconsistent. Set to threshold clp1 =< CLP0.
Relations between threshold priority1 hi and threshold priority1 low are inconsistent.	Relations between threshold priority1 hi and threshold priority1 low are inconsistent. Set the correct value.
Relations between threshold priority2 hi and threshold priority2 low are inconsistent.	Relations between threshold priority2 hi and threshold priority2 low are inconsistent. Set the correct value.
Relations between threshold priority3 hi and threshold priority3 low are inconsistent.	Relations between threshold priority3 hi and threshold priority3 low are inconsistent. Set the correct value.
Relations between threshold priority4 hi and threshold priority4 low are inconsistent.	Relations between threshold priority4 hi and threshold priority4 low are inconsistent. Set the correct value.
Relations between timeslot number and width are inconsistent.	The (timeslot number, timeslot width) value exceeds other timeslot number. Correct the (timeslot number, timeslot width) value so the value does not exceed other timeslot number.
Relations between total of vc and vp shaping number are inconsistent.	Relations between total of vc and vp shaping number are inconsistent. Set the correct value.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

Relations between total of vp and vp shaping number are inconsistent.	Relations between total of vp and vp shaping number are inconsistent. Specify the VP count to the maximum VP count of VP shaper or less.
Relations between traffic abr pcr and vp pcr are inconsistent.	Relations between traffic abr pcr and vp pcr are inconsistent. Set to PCR of PCR =< VP of ABR traffic.
Relations between traffic gfr mcr and vp pcr are inconsistent.	Relations between traffic gfr mcr and vp pcr are inconsistent. Set to MCR =< VP of GFR traffic.
Relations between traffic gfr2 mcr and vp pcr are inconsistent.	Relations between traffic gfr2 mcr and vp pcr are inconsistent. Set the correct value.
Relations between traffic gfr pcr and vp pcr are inconsistent.	Relations between traffic gfr pcr and vp pcr are inconsistent. Set to PCR of PCR =< VP of GFR traffic.
Relations between traffic gfr2 pcr and vp pcr are inconsistent.	Relations between traffic gfr2 pcr and vp pcr are inconsistent. Set the correct value.
Relations between traffic type and service category pattern are inconsistent.	Relations between traffic type and service category pattern are inconsistent. Specify the traffic type appropriate for the service category pattern.
Relations between traffic type and vp shaping number are inconsistent.	Relations between traffic type and vp shaping number are inconsistent. When the maximum VP count of VP shaper is no, specify only UBR for traffic type.
Relations between traffic vbr pcr and vp pcr are inconsistent.	Relations between traffic vbr pcr and vp pcr are inconsistent. Set to PCR of PCR =< VP of VBR traffic.
Relations between vci and vpi vci range are inconsistent.	Relations between vci and vpi vci range are inconsistent. Set VCI value within the range of VPI/VCI.
Relations between vpi and vpi vci range are inconsistent.	Relations between vpi and vpi vci range are inconsistent. Set VPI value within the range of VPI/VCI.
Relations between vpi vci range and vp shaping number are inconsistent.	Relations between vpi vci range and vp shaping number are inconsistent. Specify the value within the range of VPI/VCI to the maximum VP count of VP shaper.
RmEthernet is not supported.	Can not set rmEthernet. RmEthernet is not supported.
Scr not specified.	Scr not specified. Set SCR.
Server rate2 is greater than server rate1.	Minimum throughput rate 2 of sending to network at heavy congestion change exceeds minimum throughput rate 1 of sending to network at heavy congestion change. Specify the value so minimum throughput rate 2 of sending to network at heavy congestion change does not exceed minimum throughput rate 1 of sending to network at heavy congestion change.
The total of <item> exceeded <value>.	The total of <item> exceeded <value>. Set <item> in range.
The total of bandwidth is greater than 6144kbps.	Total of bandwidth of DLCL in the line is greater than 6144 kbps. Specify the value so the total bandwidth of DLCL in the line becomes no greater than 6144 kbps.
The total of line (same dch line is specified) exceeded 16.	The total of line (same dch line is specified) exceeded 16. Set 16 or less lines.
The total of line (same dch line is specified) exceeded 4.	The total of line (same dch line is specified) exceeded 4 (if the call number length is 4). Set 4 or less lines.
The total of line (same dch line is specified) exceeded 8.	The total of line (same dch line is specified) exceeded 8. Set 8 or less lines.
The total of line and subline (same RP is specified) exceeded 32.	The total of line and subline (same RP is specified) per 1RP exceeded 32. Set 32 or less.
the total of timeslot (pri line no. 4,5,6,7) exceeded 31.	The total of timeslot (pri line no. 4,5,6,7) exceeded 31. With the J1 line number of 4, 5, 6 or 7 and with the J1_8 line version, the total number of time slots shall not exceed 31.
The total of timeslot and line without timeslot configuration (same RP is specified) exceeded 256.	The total of timeslot and line without timeslot configuration exceeded 256. Set 256 or less.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Network Interface Error Messages (continued)

The total of traffic cbr pcr, vbr scr, and abr mcr exceeded vp pcr.	The total of traffic cbr pcr, vbr scr, and abr mcr exceeded vp pcr. Set the total traffic to VP's PCR or less.
The total of traffic gfr mcr exceeded vp pcr.	The total of traffic gfr mcr exceeded vp pcr. Set the total traffic to VP's PCR or less.
The total of traffic gfr2 mcr exceeded vp pcr.	The total of traffic gfr2 mcr exceeded vp pcr. Set the correct value.
Timeslot number not specified.	Timeslot number has not been specified. Specify a timeslot number.
Traffic not specified.	Traffic has not been specified. Specify traffic.
Tunnel interface is not defined.	Tunnel interface is not defined. The 256th interface cannot be set when a tunnel interface is defined. Reconfirm the number of IP interfaces.
Can not change tunnel type.	It is not possible to change configured tunnels to 6to4 tunnels and vice versa. Set new definitions after deleting tunnel interface information.
6to4 tunnel is already defined.	6to4 tunnel is already defined. 1 6to4 tunnel can be defined per device.
Type not specified.	Traffic type has not been specified. Specify traffic type.
Vpi not specified.	Vpi has not been specified. Specify vpi.
width is not in range of 1 to 2.	Timeslot width is not in range. Set timeslot width in range of 1 to 2.
width is not in range of 1 to 24 or not 48, 72, 96.	Timeslot width is not in range. Set timeslot width in range of 1 to 24 or 48, 72, 96.
width is not in range of 1 to 24.	Timeslot width is not in range. Set timeslot width in range of 1 to 24.
width is not in range of 1 to 31.	Timeslot width is not in range. Set timeslot width in range of 1 to 31.
Width not specified.	Timeslot width has not been specified. Specify a timeslot width.
<item> is not in range <value1> to <value2>.	<item> is not in range. Set <item> in range.
	<item> Parameter name, <value1>Minimum value <value2> Maximum value
<Option> out of range.	<Option> is out of range. Check <option>.

Downloaded from www.Manualslib.com manuals search engine

5.4 IP Information

Table 5-4 IP Information Error Messages

Message	Contents
Can not be multihome.	Only one IP address can be specified in the specified line. Specify only one IP address.
Can not change interface name.	Interface in which an IP address is set cannot be changed. To change interface, delete it and set the IP address in the target interface.
Can not delete IP configuration dlci with dlci-group replace.	There is "replace" information in the DLCI-group. Before deleting the IP information, remove "replace" from the dlci-group.
Can not delete IP configuration dlci with dlci-group.	There is group information on DLCI. Before deleting the IP information, remove DLCI from the dlci-group.
Can not delete IP configuration referred by Backup configuration.	Can not delete IP configuration referred by Backup configuration. Delete the BACKUP information first and then delete the IP information.
Can not delete IP configuration referred by bridge filtering database configuration.	Can not delete IP configuration referred by bridge filtering database configuration.Delete the target interface specification of filtering database first.
Can not delete IP configuration referred by bridge extended filtering configuration.	Can not delete IP configuration referred by bridge extended filtering configuration. Delete the target interface specification of extended filtering first and then delete the IP information.
Can not delete IP configuration referred by filter interface configuration.	IP filter list information present. Delete IP filter list information; delete the IP information.
Can not delete IP configuration referred by filter list configuration.	IP filter list information present. Delete IP filter list information; delete the IP information.
Can not delete IP configuration referred by IPX filtering configuration.	Interface specified by IPX filtering is to be deleted. After this specified interface of IPX filtering is deleted, delete the interface.
Can not delete IP configuration referred by policy list configuration.	There is information on the policy routing list. Before deleting IP information, remove the information on the policy routing list.
Can not delete IP configuration referred by QoS IP configuration.	QoS IP interface is to be deleted. Delete QoS IP interface; delete the interface.
Can not delete IP configuration referred by QoS IPX configuration.	Interface specified by QoS IPX is to be deleted. After this interface of QoS IPX is deleted, delete the interface.
Can not delete IP configuration referred by QoS bridge configuration.	Can not delete IP configuration referred by QoS bridge configuration. Delete the target interface specification of bridge first and then delete the IP information.
Can not delete IP configuration referred by QoS hdlc pasthrough configuration.	Can not delete IP configuration referred by QoS hdlc pasthrough configuration. Delete the target interface specification of passthrough first and then delete the IP information.
Can not delete IP configuration referred by Virtual Router configuration.	Virtual Router information present. Delete Virtual Router information; delete the IP information.
Can not delete IP configuration vc with vc-group.	VC group information present. Delete vc-group information; delete the IP information.
Can not delete IP configuration with ARP configuration.	ARP information present. Delete ARP information; delete the IP information.
Can not delete IP configuration with bridge interface.	Can not delete IP configuration with bridge interface. Delete the bridge interface first and then delete IP information.
Can not delete IP configuration with IP address.	An IP address exists. Delete IP address; delete IP information.
Can not delete IP configuration with IPX interface.	IP configuration with IPX interface is to be deleted. After IPX interface is deleted, delete IP configuration.
Can not delete IP configuration with relay interface configuration.	Can not delete IP configuration with relay interface configuration. Delete the relay interface information first and then delete the interface.

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 IP Information Error Messages (continued)

Can not delete policy group configuration with filter list configuration.	IP filter list information exists. Delete IP filter list information; delete policy group information.
Can not delete policy list configuration with policy group configuration.	Policy group information exists. Delete policy group information first, and delete policy group information.
Can not delete relay group configuration with relay interface configuration.	Can not delete relay group configuration with relay interface configuration. Delete the relay interface information first and then delete the relay group information.
Can not delete relay list configuration with relay group configuration.	Can not delete relay list configuration with relay group configuration. Delete the group first and then delete the list.
Can not set ARP configuration.	ARP is set in other than Ethernet, ATM, or DLCI. ARP can be set only in Ethernet, ATM, and DLCI. Delete ARP.
Can not set IP address on interface which is not configured to use IP protocol.	IP address cannot be set on the interface not configured to use IP protocol. Set IP first.
Can not set IP address on line router which is not configured to use IP protocol.	IP address cannot be set on the line router not configured to use IP protocol. Set IP first.
Can not set IP address on non-existing interface <name>.	Specified interface for IP address does not exist. Check the interface. <name> configuration information name.
Can not set IP address.	Can not set IP address. The IPv6 address cannot be set, if the interface name type of IP is "group," or if a rmEthernet, AUX, frame relay or DLCI line is used. IPv6 address settings are not permitted for an IP that has a VLAN-defined IPv4 address already set.
Can not set IP configuration on line which is not bound to IP protocol.	Attempt made to set IP on the line that is not bound to IP protocol. Set the protocol first.
Can not set IP configuration to <name>.	Attempt made to set IP in grouped interface or interface where IP is defined. Check the specified interface. <name> configuration information name.
Can not set ip null.	Can not set ip null. If 256 interfaces are set for an RP, settings are impossible. Remove the interface for the RP that has 256 interfaces set.
Can not set vlan.	Can not set vlan. VLAN can be set only on an Ethernet or a gigabit Ethernet. If both an IPv4 address and an IPv6 address are set for an IP, VLAN cannot be set for the IPv4 address on the IP.
Can not set vpn.	Can not set vpn. If PPP and the frame relay IP are defined in the same physical port, only one of either PPP or the frame relay IP can be set in VPN settings.
Change is not possible	The configuration definition cannot be changed. Set it after deleting the configuration definition.
Connect type is not point.	IP type is not point. Specify point to the IP type.
Destination ip address not specified.	Although connection type is point-to-point, a destination address has not been specified. Or, the PPP line is set or an IPv6 address other than linklocal is set for TUNNEL. However, settings are not made for the destination address. Specify destination address.
Duplicate destination IP address.	The same destination IP address is set. Make each destination IP address unique.
Duplicate interface name and next hop address.	The policy list set has the interface name and the next hop address with the same contents. Make all policy lists unique.
Duplicate IP address.	The same IP address is used. Make each IP address unique.
Duplicate network address.	IP address of the same network address is defined. Specify an IP address so that each network address becomes unique.
Duplicate policy group configuration.	Duplicate policy group configuration. Make settings so that each policy group entry has unique contents.
Duplicate pool ip address.	The same pool IP addresses are set in the same RP. Make settings so that pool addresses in the same RP are unique.
Duplicate prefix.	Duplicate prefix IP address. Set prefix to unique.

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 IP Information Error Messages (continued)

Duplicate relay address.	Duplicate relay address. Set all of the DHCP relay addresses to unique.
Duplicate subject IP address.	The same IP address is used. Make each IP address unique.
Duplicate vlan.	The same VLANs are set in the same physical port. Make settings so that VLANs in the same RP are unique.
Inconsistency has occurred in a setting of IPv6 address and NDP.	There is a conflict in the prefixes between the address set by the IP information and the address set by the NDP information. Designate the address prefixes correctly.
Interface name not specified.	Interface name not specified. Set interface name. Enter a correct interface name.
Invalid connect type.	The connection type is illegal. On an ATM or ISDN PPP line, if the connection type is "broadcast," you cannot set IPv6.
Invalid critical interface name.	The error monitoring interface name is illegal. For the error monitoring interface name, use a name other than AUX.
Invalid destination IP address.	Destination IP address value invalid. Set a correct destination IP address
Invalid host address.	Host address is 0 or ALL 1. Specify the value so host address is neither 0 nor ALL 1.
Invalid IP address.	IP address value invalid. Set a correct IP address.
Invalid name <name>.	Entered name of configuration information invalid. For group: Specify DLCI name on the same RP already defined. For PPP, frame relay: Specify line name whose line type is serial, oc3pos, oc12pos, or name of timeslot. For DLCI: Specify name set in frame relay. For timeslot: Specify line name whose line type is pri, j2, bri. For filter interface, qos ip: Specify line name of the line where IP is set. For QoS interface: Specify name set in ethernet, frame relay, dlci, ppp. For IP: Specify name set in ethernet, frame relay, dlci, ppp, vc, ISDN PPP, Group, Tunnel. For ARP: Specify name set in ethernet, dlci, vc, ISDN PPP. For Virtual Router: Specify the name of a line other than AUX for which the IP is set. For Policy List: Specify the name of a line other than rmEthernet and AUX for which an IP is set. For Relay Interface: RmEthernet for which an IP is set. Specify an interface name other than AUX. <name>configuration information name
Invalid network class.	IP address network class does not match subnet mask network class. Correct IP address network address and subnet mask class.
Invalid policy routing interface name.	Policy routing interface name is invalid. For the name of the interface for policy routing, use a name other than AUX.
IP address is duplicate between interface and static NDP entry.	The address set by the IP information is duplicated with the address set by the NDP information. Designate the addresses without duplication.
IP address not specified.	IP address has not been specified. Specify an IP address.
IP configuration not specified.	IP routing has not been specified. Specify IP routing.
IP configuration not specified.	IP routing has not been specified. Specify IP routing.
IP interface is not defined.	You are about to set the relay interface without IP routing. Before setting the relay interface, make IP routing settings.
MAC address not specified.	MAC address has not been specified. Specify MAC address.
Maximum number of IP address are already defined.	No more IP address can be set. Check the network configurations.

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 IP Information Error Messages (continued)

Maximum number of IP addresses are already defined on the RP.	Number of IP addresses exceeded maximum value. Decrease number to 256 per RP.
Maximum number of IP configurations are already defined.	No more IP configurations can be set. Check the network configurations.
Maximum number of linklocal address are already defined.	No more linklocal address can be set. Check the network configurations.
Maximum number of policy group name are already defined.	Maximum number of policy groups (256) are already defined. Check the network configuration.
Maximum number of relay group name are already defined.	Maximum number of policy groups (256) are already defined. Check the network configuration.
Maximum number of Vpn Name configurations are already defined.	VPN Name can be set no more. Reconfirm the network configuration.
Network address of IP address is different from network address of broadcast address.	Network address of IP address is different from network address of broadcast address. Specify the value so the network address of IP address becomes the same as the network address of broadcast address.
Next hop address not specified.	Next hop address is not specified. Set next hop address number.
No such dhcp-client interface <Interface_Name>	The designated interface information is not available. Designated the name of the designated interface information. Interface name attached to the <Interface_Name> configuration defining information.
No such insert index.	An entry cannot be inserted on specified entry number. Set entry number not exceeding the number of set entries.
No such interface <Interface_Name> send dhcp-client-id	The designated interface's "send dhcp-client-id" information is not available. Designated the defining information's name of the designated interface information. Interface name attached to the <Interface_Name> configuration defining information.
No such interface <Interface_Name> send host-name	The designated interface's "send dhcp-host-id" information is not available. Designated the defining information's name of the designated interface information. Interface name attached to the <Interface_Name> configuration defining information.
No such line router.	No line router is set. Set the line router first.
No such name <name>.	Specified configuration information name not found. Specify existing definition information name. <name> configuration information name.
No such policy list number.	No policy list number is set. Set the policy list number.
No such relay group name.	No such relay group name. Specify DHCP relay group that has been set.
No such relay list number.	No such DHCP relay address entry. Specify DHCP relay address entry that has been set.
No such set index.	An entry cannot be set on specified entry number. Use entry number not exceeding the set number of entries. To add entries, use the number of set entries +1 for entry value.
Null interface already defined.	Null interface is already defined. Check the interface that is set.
Only the interface name can be set to the interface used for l2transport.	It is only possible to set the interface name in interfaces used in EoMPLS L2 transports.
Policy group name not specified.	Policy group name is not specified. Set policy group name.
Policy list not specified.	Policy list is not specified. Set policy list.
Policy list number not specified.	Policy list entry number is not specified. Set policy list entry number.
Reject object, dhcp-client	The configuration defining information for the DHCP client cannot be set. Confirm the configuration defining information.
Reject object, nat	The configuration defining information for the NAT cannot be set. Confirm the configuration defining information.
Relations between connect type and backup interface in backup configuration are inconsistent.	Relations between connect type and backup interface in backup configuration are inconsistent. Specify point to the connect type of interface specified by backup destination interface.

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 IP Information Error Messages (continued)

Relations between destination ip address and local address in router configuration are inconsistent.	Relations between destination ip address and local address in router configuration are inconsistent. For the IP address of the destination server (for IP without VPN defined), set an address different from the local address for router information.
Relations between destination IP address and IP address in IP address configuration.	Relations between destination IP address and IP address in IP address configuration are inconsistent. Reconfirm the set address.
Relations between external destination ip address and line type are inconsistent.	Relations between external destination ip address and line type are inconsistent. The line that can set external destination IP address is Ethernet only.
Relations between external destination ip address and obn type are inconsistent.	Relations between external destination ip address and obn type are inconsistent. When specifies external destination IP address, set OBN line type to subscriber.
Relations between external source ip address and obn type are inconsistent.	Relations between external source ip address and obn type are inconsistent. When specifies external own IP address, set OBN line type to subscriber or dps.
Relations between IP address and destination IP address are inconsistent.	Relations between Ipv6 address and destination Ipv6 address are inconsistent. For IPv6 and destination IPv6, set a different address.
Relations between ip address and local address in router configuration are inconsistent.	Relations between ip address and local address in router configuration are inconsistent. For the IP address of the destination server (for IP without VPN defined), set an address different from the local address for router information.
Relations between IP address and target address in VirtualRouter configuration are inconsistent.	The IP address and Virtual Router target address are inconsistent. Reconfirm the address setting.
Relations between next hop address and destination IP address in IP configuration.	Relations between next hop address and destination IP address in IP configuration are inconsistent. Reconfirm the set address.
Relations between obn type and line type are inconsistent.	Relations between obn type and line type are inconsistent. The line that can specify subscriber is other than Gigabit Ethernet, ATM, or frame relay. The line that can specify dps is Ethernet only.
Relations between obn type and proxy arp are inconsistent.	Relations between obn type and proxy arp are inconsistent. When specifies subscriber or dps, set ARP proxy response switch to off.
Relations between physical interface type and backup interface in backup configuration are inconsistent.	Relations between physical interface type and backup interface in backup configuration are inconsistent. Check interface type in backup interface. The relationship between the interface type and the interface at the backup server. Recheck the interface type of the interface at the backup server.
Relations between policy routing IP address and destination IP address in IP configuration.	Relations between policy routing IP address and destination IP address in IP configuration are inconsistent. Reconfirm the set address.
Relations between vpn in IP configuration and backup interface.	Relations between vpn in IP configuration and backup interface are inconsistent. Reconfirm vpn in IP or the backup interface.
Relay address not specified.	Relay address not specified. Set DHCP relay address.
Relay group name not specified.	Relay group_name not specified. Set relay group name.
Relay group not specified.	Relay group not specified. Set DHCP relay group first.
Relay list not specified.	Relay list not specified. Set DHCP relay list first.
Relay list number not specified.	Relay list number not specified. Set DHCP relay address entry number.
Subject IP address not specified.	IP address is not specified. Set IP address.
Subnet mask not specified.	Subnet mask has not been specified. Specify a subnet mask.
The interface is neither ethernet nor gigabit ethernet.	The interface is neither ethernet nor gigabit ethernet. Specify interface of Ethernet or Gigabit Ethernet.
The total of interfaces exceeded 256.	The total of interfaces exceeded 256. Set 256 or less lines.
The total of policy list entry (default is specified in same policy group) exceeded 1.	The total number of default-designated policy list entries inside a policy group has exceeded "1." Set the number below 1.

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 IP Information Error Messages (continued)

This interface is multihome/please use ip-address object.	Because this interface is configuration information of multihome, it cannot be set. Set by using ip-address object.
Virtual router ip address not specified.	Virtual router ip address not specified. Set Virtual router ip address.
Cannot utilize IPv6 and VPN option simultaneously.	It is not possible to simultaneously set IPv6 addresses and VPN IDs. Do not set them simultaneously.
6to4 tunnel configuration is already defined.	An IPv6 address is already set in the 6to4 tunnel. It is not possible to set multiple IPv6 addresses in a 6to4 tunnel.
Invalid 6to4 tunnel IPv6 address.	The address defined in the 6to4 tunnel is invalid as an IPv6 address. It is not possible to set IPv4 addresses in 6to4 tunnels.
IPv4 address cannot change because used by 6to4 tunnel.	It is not possible to change since it is an IPv4 address contained in the IPv6 address of the 6to4 tunnel. First change the IPv6 address of the 6to4 tunnel or delete the configuration definition of the 6to4 tunnel.
IPv4 address cannot delete because used by 6to4 tunnel.	It is not possible to delete since it is an IPv4 address contained in the IPv6 address of the 6to4 tunnel. First change the IPv6 address of the 6to4 tunnel or delete the configuration definition of the 6to4 tunnel.
IPv4 address not defined.	The IPv4 address contained in the IPv6 address of the 6to4 tunnel that you attempted to define is not defined. When defining 6to4 tunnels, specify an IPv6 address containing an IPv4 address that is already defined.
IPv4 address is not global or not unicast.	The IPv4 address contained in the IPv6 address of the 6to4 tunnel that is being defined is not a global address. When defining 6to4 tunnels, specify an IPv6 address containing a global unicast IPv4 address.
6to4 address is invalid. 6to4 address must start "2002".	The IPv6 address of the 6to4 tunnel that is being defined does not begin with 2002. Use an address with the prefix 2002::/16 for the IPv6 address specified in the 6to4 tunnel.

Downloaded from www.Manualslib.com manuals search engine

5.5 Routing Protocol

Table 5-5 Routing Protocol Error Messages

Message	Contents
aggregate: duplicate AS path pattern in list	In the aggregate definition, an AS path is duplicated. Specify a unique AS path.
aggregate: duplicate autonomous-system in list at <As>	In the aggregate definition, an AS number is duplicated. Specify a unique AS number.
	<As>: Specified AS number
aggregate: duplicate entry at <Address> mask <Mask> [exact | refine]	In the aggregate definition, a network range is duplicated. Specify a unique network range.
	<Address>: Specified address <Mask>: Specified Mask
aggregate: duplicate tag in last at <Tag>	In the aggregate definition, a tag is duplicated. Specify a unique tag.
	<Tag>: Specified tag
aggregate: invalid autonomous system value at <value> not in range 1 to 65534	AS number is invalid. Specify a value within the range of 1 to 65534.
	<Value>: Specified AS number
aggregate: invalid external-route-tag value at <Value> not in range 0 to 2147483647	AS external-route tag value is invalid. Specify a value within the range of 0 to 2147483647.
	<Value>: Specified AS external route number
aggregate: invalid high end of range value at <Value> not in range 0 to {32|128}	In the between specification, upper limit value of a mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Upper limit value of the specified mask range
aggregate: invalid {inet|IPv6} mask bits value at <Value> not in range 0 to {32|128}	At masklen/prefixlen, the mask length is invalid. Specify a value within the range of 0 to 32/128.
	<Masklen>: Specified mask length
aggregate: invalid low end of range value at <Value> not in range 0 to {32|128}	In the between specification, lower limit value of a mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Lower limit value of the specified mask range
aggregate: invalid number of communities value at <Value> not in range 0 to 25	Specified community count is over the limit. Specify a value of up to 25.
	<Value>: Specified number of communities
aggregate: invalid octet value at <Value> not in range 0 to 255	Specified community count is over the limit. Specify a value of up to 25.
	<Value>: Specified value
aggregate: invalid preference value at <value> not in range 0 to 255	Preference value is invalid. Specify a value within the range of 0 to 255.
	<Value>: Specified preference value
aggregate: invalid range end: <Value>	With aspath_term {m, n} specified, m>n or n is 256 or more. Set the starting value below the ending value. Or, set the ending value to 255 or less.
	<Value>: Specified ending value (n)
aggregate: invalid range start: <Value>	With aspath_term{m,n}, {m}, {m,} specified, m is 256 or more. Set to 255 or less.
	<Value>: Specified starting value (m)
aggregate: invalid vpn number value at <Value> not in range 1 to <Max_Value>	VPN number is invalid. Specify a value within the range of 1 to <Max_Value>.
	<Value>: Specified VPN number <Max_Value>: Maximum VPN number
aggregate: iPv6 prefix cannot be linklocal in configuration.	Linklocal address is specified in network address. Do not use the linklocal address.
aggregate: iPv6 prefix cannot be multicast in configuration.	Multicast address is specified in network address. Do not use the multicast address.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

aggregate: linklocal address should be followed by % (IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
aggregate: low end of range <Mask1> shorter than prefix mask <Mask2>	In the between specification, lower limit value of the mask range is overlapped with specified mask. Specify the value so that mask range does not overlap with specified mask.
	<Mask1>: Lower limit value of the specified mask range. <Mask2>: Specified mask.
aggregate: low end of range (<Value1> bits) is greater than high end (<Value2> bits)	In the between specification, lower limit value of the mask range is greater than upper limit value. Reduce lower limit value of the mask range to less than upper limit value.
	<Value1>: Lower limit value of the mask range <Value2>: Upper limit value of the mask range
aggregate: mask not contiguous	Bit 1 of specified mask does not continue. Use a mask where bit 1 continues.
aggregate: Non-masked bits not zero for <Address> mask <Mask>	At mask, 1 is set to non-masked bit of specified address. Set non-masked bit 0.
	<Address>: Specified Address <Mask>: Specified Mask.
aggregate: Non-masked bits not zero for <Address> masklen <Masklen>	t masklen, 1 is set to non-masked bit of specified address. Set non-masked bit 0.
	<Address>: Specified address <Masklen>: Specified Mask length
aggregate: not IPv6 prefix.	Addresses other than an IPv6 prefix are specified. Specify IPv6 prefix.
aggregate: out of range.	Input *syntax* command
aggregate: syntax error	Syntax error
attribute-list: attribute-list name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
attribute-list: duplicate Attribute-filter at <Value>	The specified ID number has been already registered. Specify the other ID number.
	<Value>: ID number.
attribute-list: duplicate extended community.	The extended community is duplicated for definition. Do not duplicate the extended community for definition.
attribute-list: duplicate Set-attribute at <Value>	The specified ID number has been already registered. Specify the other ID number
	<Value>: ID number
attribute-list: error resolving' <Host Name>': Unknown host.	The specified host name is not found. Specify the defined host name.
	<Host Name>: Specified host name
attribute-list: invalid as_count value at <Value> not in range 1 to 25	The specified ascount value is invalid. Specify within the range of 1 to 25.
	<Value>: Specified ascount value.
attribute-list: invalid attribute-list number value at <Value> not in range 1 to 65535	The specified ID number is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified ID number.
attribute-list: invalid autonomous system number value at <Value> not in range 1 to 65534	The AS number is invalid in the extended community. Specify within the range of 1 to 65534.
	<Value>: Specified As value.
attribute-list: invalid autonomous system value at <Value> not in range 1 to 65534	The AS number is invalid. Specify within the range of 1 to 65534.
	<Value>: Specified As value.
attribute-list: invalid { BGP | BGP4+ } metric offset value at <Metric> not in range 1 to 4294967295	The range for specifying MED offset values is invalid. Specify within the range of 1 - 4294967295.
	<Metric>: Specified MED offset value

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

attribute-list: invalid {BGP|BGP4+} metric value at <Metric> not in range 0 to 65535	The specified MED number is invalid. Specify within the range of 0 to 65535.
	<Metric>: Specified MED number.
attribute-list: invalid index number in extended community number value at <Value> not in range 0 to { 65535 | 4294967295 }	The extended community ID number is invalid. Specify within the range of 1 to 65535, or 0 to 4294967295.
	<Value>: Specified ID number.
attribute-list: invalid localpref offset value at <Localpref> not in range 1 to 65535	The specified LOCALPREF offset number is invalid. Specify within the range of +1 to +65535 or -1 to -65535.
	<Localpref>: Specified LOCALPREF offset number
attribute-list: invalid localpref value at <Localpref> not in range 0 to 65535	The specified LOCALPREF number is invalid. Specify within the range of 0 to 65535.
	<Localpref>: Specified LOCALPREF number
attribute-list: invalid number of aspath value at <Value> not in range 1 to 8	The specified ASPATH value is invalid. Specify within the range of 1 to 8.
	<Value>: Specified ASPATH number
attribute-list: invalid number of communities value at <Value> not in range 0 to 25	The specified community count is over. Specify a value of 25 or less.
	<Value>: Specified communities value
attribute-list: invalid number of extended communities value at <Value> not in range 0 to 25.	The number of extended communities to be defined exceeds the maximum number of extended communities to be defined. Specify a value of 25 or less.
	<Value>: Extended communities value.
attribute-list: invalid octet value at <Value> not in range 0 to 255.	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
attribute-list: invalid range end: <Value>	m>n or n is 0 in specifying of aspath_term {m ,n}. Specify the starting value smaller than the terminating value. Or, specify terminating value to other than 0.
	<Value>: Specified terminating value (n)
attribute-list: invalid range start: <Value>	m is 0 in specifying of aspath_term {m, n}, {m}, {m,}. Specify other than 0.
	<Value>: Specified starting value (m)
attribute-list: out of range	The parameter-specified range is exceeded in the *input* command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
attribute-list: syntax error	Syntax error
autonomoussystem: autonomous-system already specified	The autonomoussystem definition is duplicated. Delete one of the two.
autonomoussystem: invalid autonomous system value at <Value> not in range 1 to 65534	AS number specification range is illegal. Specify value within the range of 1 to 65534.
	<Value>: Specified As number
autonomoussystem: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
autonomoussystem: syntax error	Syntax error
autonomoussystem6: autonomous-system already specified	The autonomoussystem6 definition is duplicated. Delete one of the two.
autonomoussystem6: invalid autonomous system value at <Value> not in range 1 to 65534	IPv5 AS number specification range is illegal. Specify value within the range of 1 to 65534 <Value>: Specified As number
autonomoussystem6: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
autonomoussystem6: syntax error	Syntax error

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp: as-count only makes sense with external peers	The ascount parameter is specified in a peer other than an external peer. Do not specify the ascount parameter in an internal or routing peer.
bgp: as-count option is not supported the policy group	as-count option is specified by policy group. Specify the option from export filter side
bgp: as-override may only be used with external peers	The AS-override option is set for other than an external peer. The AS-override option may only be used for the external peer.
bgp: as-override option must be the same in the policy group	Different AS-override options are used in the policy group. Use the same AS-override option within the policy group.
bgp: aspath-opt option is not supported the policy group	aspath-opt option is specified by policy group. Specify the option from export filter side
bgp: authmd5 must be equal to or greater than one character	The designated authentication key is less than one character. Designate the authentication key using between 1 and 80 characters.
bgp: authmd5 "<MD5>" longer than 80 characters	The designated authentication key is longer than 80 characters. Designate the authentication key by using less than 80 characters.
	<MD5> Designated authentication key.
bgp: autonomous-system not specified	AS number of this router has not been defined Define the AS number of the local router before specifying member AS number
bgp: autonomous-system not specified, and it is required for BGP	AS number of this router has not been defined. Define the AS number of the local router.
bgp: capability option must be specified ipv4-uni or ipv4-vpn	In the capability option, neither ipv4-uni nor ipv4-vpn is defined. When the capability option is specified, define ipv4-uni or ipv4-vpn.
bgp: capability option must be specified ipv4-vpn	The ipv4-vpn is not defined by the local peer's capability option. When designating the capability option, define the ipv4-vpn.
bgp: clusterid may not be 0.0.0.0	0.0.0.0 is specified to cluster ID. Use a value other than 0.0.0.0.
bgp: clusterid option not valid for vpn	The clustered option is defined for VPN. VPN does not support this.
bgp: confederation peer must have the member AS	For settings of member-to-member peers, a member AS is essential. Specify a member AS.
bgp: description "<Name>" longer than 64 characters	The specified ID exceeds 64 characters. Specify ID by 64 or less characters.
	<Name>: Specified identifier
bgp 4: description may only be used in peers.	description option is defined by peer group. Define the description option is peer.
bgp: duplicate bgp clause	A bgp definition is duplicated. Delete one of the two.
bgp: duplicate BGP group found, groups must differ by type and/or AS	The same peer group is already defined. Use a unique peer group.
bgp: duplicate entries for peer <Address> found in group type <Type> AS <As>	The same peer is specified. Specify a different peer.
	<Address>: Specified peer address <Type>: Specified peer group <As>: Specified peer group AS number
bgp: error resolving '<Host Name>': Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host name>: Specified host name
bgp: external peer must not have the same AS as we do locally (<As>)	Peer AS number of external peer is the same as local router AS number. Do not specify AS number of the local router in the peer AS number of external peer.
	<As>: Local router AS number

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp: external peer must not have the same AS as we do locally member AS (<As>)	Peer AS number of external peer is the same as local router AS number. Do not specify AS number of the local router in the peer AS number of external peer.
	<As>: Local router member AS number>
bgp: gateway not a host address on an attached network : <Address>	Specified gateway is not the host address on the connected network. Specify gateway address on the defined interface address.
	<Address>: Specified gateway address
bgp: gateway option is not supported for this peer type	The gateway option is designated in the local peer. Do not designate the gateway option in the local peer.
bgp: holdtime option is not supported for this peer type	The holdtime option is designated in the local peer. Do not designate the holdtime option in the local peer.
bgp: ignorefirstashop option is not supported for this peer type	The ignorefirstashop option is designated in the local peer. Do not designate the ignorefirstashop option in the local peer.
bgp: Interface not found at <Address>	Interface at the specified interface address is not found. Use a defined interface address.
	<Address>: Specified interface address
bgp: interfaces may only be specified for internal routing groups	Interface parameters are specified for other than routing peers. Do not specify an interface parameter for other routing peers.
bgp: invalid as_count value at <Value> not in range 1 to 25	AS count value is invalid. Specify a value within the range of 1 to 25.
	Ascount<Value>: Specified account value
bgp: invalid autonomous system value at <Value> not in range 1 to 65534	AS number is invalid. Specify a value within the range of 1 to 65534.
	<Value>: Specified AS number
bgp: invalid BGP metric value at <Metric> not in range 0 to4294967295	In the BGP definition, BGP metric is invalid. Specify a value within the range of 0 to 4294967295.
	<Metric>: Specified metric value
bgp: invalid community id value at <Value> not in range 0 to 65535	In the comm-split parameter, the range of Comm_id value is invalid. Specify a value within the range of 0 to 65535.
	<Value>: Specified Comm_id value
bgp: invalid hold time value at <Value> not in range 0 to 65535	Hold timer is invalid. Specify a value within the range of 0 or 3 to 65535.
	<Value>: Specified hold timer value
bgp: Invalid interface at <Address>	Interface at the specified interface address (lcladdr parameter in bgp) is not found. Use a defined interface address.
	<Address>: Specified interface address
bgp: invalid lcladdr at <Address>	The interface address of the designated leladdr parameter is incorrect.
	<Address>: Specified interface address
bgp: invalid number of communities value at <Value> not in range 0 to 25	Specified community count is over the limit. Specify a value of 25 or less.
	<Value>: Specified communities value
bgp: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
bgp: invalid policy group number value at <Group Number> not in range 1 to 16	The specified policy group number is invalid. Specify within the range of 1 to 16.
	<Group Number>: Specified masklen
bgp: invalid preference value at <Value> not in range 2 to 255	Preference value is invalid. Specify a value within the range of 0 to 255.
	<Value>: Specified preference value
bgp: invalid seconds value at <Value> not in range 0 to 4294967295	Timer value is invalid. Specify a value within the range of 0 to 4294967295.
	<Value>: Specified timer value

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp: invalid ttl value at <Value> not in range 1 to 255	The specified TTL value is invalid. Specify within the range of 1 to 255.
	<Value>: Specified TTL value
bgp: invalid vpn number value at <Value> not in range 1 to <Max_Value>	The specified VPN number value is invalid. Specify within the range of 1 to <Max_Value>.
	<Value>: Specified vpn number <Max_Value>: Maximum VPN number
bgp: ipv4-uni option is not supported for this peer type	The local peer has the ipv4-uni option designated. Do not designate the ipv4-uni option in the local peer.
bgp: ipv4-vpn option not valid for vpn	The Ipv4-vpn option is defined for VPN. This option may only be defined for other than VPN.
bgp: keep-none-vpn option not valid for vpn	The Keep-none-vpn option is defined for VPN. This option may only be defined for other than VPN.
bgp: lcladdr option is not supported for this peer type	The local peer has the lcladdr option designated. Do not designate the lcladdr option in the local peer.
bgp: local-as may only be used with external peers	The Local-as option is defined for other than external peers. This option may only be used for external peers.
bgp: local-as option is not supported for this peer type	The local peer has the local-as option designated. Do not designate the local-as option in the local peer.
bgp: member-as must be different autonomous-system	The number of AS to which this system belongs is the same as the member AS. Specify different numbers for AS and member AS.
bgp: member-as option not valid for vpn	The Member-as option is defined for VPN. VPN does not support confederation.
bgp: metric-out option is not supported the policy group	metricout option is specified by policy group. Specify the option from export filter side.
bgp: multihop option is not supported for this peer type	The local peer has the multihop option designated. Do not designate the multihop option in the local peer.
bgp: multipath option not valid for vpn route	The Multipath option is defined for VPN. VPN does not support the multipath option.
bgp: multipath-option (all-as) must be set compare-med (all-as)	Multipath-option (all-as) must be set compare-med (all-as). When specifies all-as parameter of multipath-option, specify all-as parameter of compare-med.
bgp: nexthopself option is not supported for this peer type	The local peer has the nexthopsel option designated. Do not designate the nexthopsel option in the local peer.
bgp: nogendefault option is not supported for this peer type	The local peer has the nogendefault option designated. Do not designate the nogendefault option in the local peer.
bgp: No Router ID has been assigned for comparison to peer <Peer>	No router ID is defined. Define a router ID.
	<Peer>: Specified peer
bgp: Number of local-as is more than maximum permited(16)	Number of local-as is more than maximum permited (16). Specify maximum number of local-as of 16 or less.
bgp: Only External groups may be Confederation Peer	The confederation parameter is specified for the internal peer. Do not designate a confederation for the internal peer.
bgp: Only Internal, IGP or Routing groups may be route reflection clients	In the external peer, a reflector-client parameter is specified. In the external peer, do not specify a reflector-client parameter.
bgp: only one choice the gateway option or the setnexthoppeer option	The gateway parameter and the setnexthoppeer parameter are specified at the same time. Specify either the gateway parameter or the setnexthoppeer parameter.
bgp: only one choice the refresh option or the refresh-128 option	refresh and refresh-128 parameters are specified simultaneously. Specify a refresh or refresh-128 parameter.
bgp: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
bgp: passive option is not supported for this peer type	The local peer has the passive option designated. Do not designate the passive option in the local peer.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp: "peer local" can be used only with routing peer group	A local peer is designated somewhere other than in the routing peer. Always designate the local peer in the routing peer.
bgp: permit-asloop may only be used with external peers	The permit-asloop option is defined for other than external peers. This option can only be used for external peers.
bgp: policygroup can be used in same group type	The settings of confederation parameters in the policy group are different. The settings of confederation parameters in the policy group must be the same.
bgp: policy-group may only be used with external groups	Policy group is specified by other than external peer. The group cannot be used by other than external peer.
bgp: policy-group should be used in the group declaration only	Policy group is specified by other than peer group. Specify the group as peer group option.
bgp: remove-private-as may only be used with external peers	remove-private-as parameter is specified by other than external peer. The parameter cannot be used by other than external peer.
bgp: remove_private_as option must be the same in the policy group	The settings of remove-private-as parameters in the policy group are different. The settings of remove-private-as parameters in the policy group must be the same.
bgp: setnexthoppeer option is not supported for this peer type	The local peer has thesetnexthoppeer option designated. Do not designate the setnexthoppeer option in the local peer.
bgp: show-warnings option is not supported for this peer type	The local peer has the show-warnings option designated. Do not designate theshow-warnings option in the local peer.
bgp: site of vpn may only be used external peers	Site of vpn is specified by other than external peer. Site of vpn cannot be used by other than external peer.
bgp: syntax error	Syntax error
bgp: the BGP member AS (<As1>) and peer AS (<As2>) must be the same for internal peers	The AS No. of the internal peer does not agree with the memberAS number of the local device. As the AS No. of the internal peer and the routing peer, specify the memberAS No. of the local device.
	<As1>: memberAS No. of the local device <As2>: AS No. of the remote device.
bgp: the holdtime for BGP group peers (<Value>) is less than the minimum permitted (3)	In the BGP peer group, specified hold timer value is less than minimum value permitted. Use a value of 0 or 3 or more.
	<Value>: Specified hold timer
bgp: the holdtime for BGP peer <Address> (<Value>) is less than the minimum permitted (3)	Hold timer value of specified peer is less than minimum value permitted. Use 0 or 3 or more.
	<Address>: Specified peer address <Value>: Specified hold timer value
bgp: the IGP protocol must be specified for routing peers using the proto option	For the routing peer, a proto parameter has not been specified. For the routing peer, a proto parameter is essential. Specify a proto parameter.
bgp: the lcladdr option should be used in the group declaration only	The lcladdr parameter is different from that specified in the peer group. Specify same lcladdr parameter in internal peer and routing peer.
bgp: the local as can not be used in confederation	The local-as is specified by other than external peer. The local-as cannot be used by other than external peer
bgp: the metricout option should be used in the group declaration only	The metricout parameter is different from that specified in the peer group. Specify same metricout parameter in internal peer and routing peer.
bgp: the peer group option must be the same for policy group	The settings of peer group option in the policy group are different. The settings of peer group option in the policy group must be the same.
bgp: The peeras for an internal-type group does not match the AS number of this router	Peer AS number for an internal peer is different from AS number of local router. Specify local router AS number for peer AS numbers of internal peer and routing peer.
bgp: the proto option may only be used for internal routing groups	Proto parameter is specified in a peer other than a routing peer. Proto parameter is valid only for a routing peer.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp: This peer address <Peer> matches the local router id <Address>	Peer address is the same as router ID of local router. Specify a peer address different from router ID.
	<Peer>: Specified peer address <Address>: Local router ID
bgp4+: address should not be::	Default address is specified in address. Specify addresses other than the local host address.
bgp4+: address should not be v4-compat	An IPv4-compatible address is specified in an address. Specify addresses other than the IPv4-compatible address.
bgp4+: address should not be v4-mapped	An IPv4 mapped address is specified in an address. Specify addresses other than the IPv4 mapped address.
bgp4+: as-count only makes sence with external peers	An as-count parameter is specified using peers other than the external peer. Do not specify the as-count parameter using an internal peer and routing peer.
bgp4+: as-count optionis not supported the policy group	An as-count option is specified in the policy group. Specify an as-count option on the Export filter side.
bgp4+: as-override may only be used with external peers	An as-override option is defined in peers other than the external peer.
	An as-override option can be used only in the external peer.
bgp4+: as-override option must be the same in the policy group	as-override options are different in the policy group. as-override options must be the same in the policy group.
bgp4+: aspath-opt option is not supported the policy group	An Aspath-opt option is specified in the policy group. Specify an Aspath-opt option on the Export filter side.
bgp4+: authmd5 must be equal to or greater than one character	The designated authentication key is less than one character. Designate the authentication key using between 1 and 80 characters.
bgp4+: authmd5 "<MD5>" longer than 80 characters	The designated authentication key is longer than 80 characters. Designate the authentication key by using less than 80 characters.
	<MD5> Specified authentication key.
bgp4+:autonomous-system not specified	The AS number to which this router belongs is not defined. Define the AS number of a local router.
bgp4+: BGP4+ local-address <IPv6 Prefix> is not global/site-local IPv6 address	Defined lcladdr is except a global address or site local address. Define a global address or site local address in lcladdr.
	<IPv6 Prefix>: Specified local address
bgp4+: clusterid may not be 0.0.0.0	0.0.0.0 is specified in cluster ID. Specify cluster ID by except 0.0.0.0.
bgp4+: confederation peer must have the member AS	Setting the peer between members requires the member AS number. Specify the member AS number.
bgp4+: description "<Name>" longer than 64 characters	The specified ID exceeds 64 characters. Specify ID by 64 or less characters.
	<Name>: Specified identifier
bgp4+: description may only be used with peers	The description option is specified by other than peer group. The option for description shall be defined in the peer.
bgp4+: disable may only be used with peers	The disable option is specified by other than peer. The option for disable shall be defined in the peer.
bgp4+: duplicate bgp4+ clause	The same peer was duplicated for definition. Do not define the same peer.
bgp4+: duplicate BGP4+ group found, groups must differ by type and/or AS	Bgp4+ is double-defined. Delete one of the definitions.
bgp4+: duplicate entries for peer <Peer> found in group type <Type> AS <As>	The same peer was duplicated for specification. Do not specify the same peer.
	<Peer>: Specified peer address <Type>: Specified peer group <As>: AS number of specified peer group

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp4+: external peer must not have the same AS as we do locally (<As>)	The AS number of a local router was specified using the peer AS number of an external peer. Do not specify the AS number of a local router in the peer AS number of an external peer.
	<As>: AS number of local router
bgp4+: external peer must not have the same AS as we do locally member AS (<As>)	The member AS number of a local router was specified using the peer AS number of an external peer. Do not specify the member AS number of a local router in the peer AS number of an external peer.
	<As>: Member AS number of local router
bgp4+: gateway <IPv6 Prefix> is not global/ site-local/linklocal IPv6 address	Specified gateway is invalid. Specify the global address, site-local address or linklocal address.
	<IPv6 Prefix>: Specified gateway address
bgp4+: gateway not a host address on an attached network:<IPv6 Prefix>	The specified gateway is not a host address in the connected network. Define the gateway address in the defined interface address.
	<IPv6 Prefix>: Specified gateway address
bgp4+: Invalid address specified at lcladdr option	The interface of the specified interface address cannot be found. Specify the defined interface address.
bgp4+: invalid as_count value at '<Value>' not in range 1 to 25	The range of the Ascount value is specified incorrectly. Specify in the range of 1 to 25.
	<Value>: Specified ascount value
bgp4+: invalid BGP4+ localpref value at '<Metric>' not in range 0 to 65535	Specified LOCALPREF value is invalid. Specify value within the range of 0 to 65535.
	<Metric>: Specified LOCALPREF value
bgp4+: invalid BGP4+ metric value at '<Metric>' not in range 0 to 4294967295	BGP metric value is invalid in BGP4+. Specify value within the range of 0 to 4294967295.
	<Metric>: Specified metric value
bgp4+:invalid community id value at '<Value>' not in range 0 to 65535	In the comm-split parameter, the range of Comm_id value is invalid. Specify a value within the range of 0 to 65535.
	<Value>: Specified Comm_id value
bgp4+: invalid hold time value at '<Value>' not in range 0 to 65535	Hold time value is invalid. Specify value within the range of 3 to 65535 or 0.
	<Value>: Specified ascount value
bgp4+: invalid policy group number value at <Group Number> not in range 1 to 16	Policy group number is invalid. Specify a value within the range of 1 to 16.
	<Group Number>: Specified masl length
bgp4+: invalid preference value at '<Value>' not in range 2 to 255	Preference value is invalid. Specify value within the range of 2 to 255.
	<Value>: Specified preference value
bgp4+: local-as may only be used with external peers	The Local-as option is defined for other than external peers. This option may only be used for external peers.
bgp4+: member-as must be different autonomous-system	The AS number to which this device belongs is the same as the member AS number. Specify the AS number with a different number from the member AS number.
bgp4+: metric-out option is not supported the policy group	A Metricout option is specified in the policy group. Specify a Metricout option on the Export filter side.
bgp4+: multipath-option (all-as) must be set compare-med (all-as)	For the all-as parameter of multipath-option, the all-as parameter of compare-med must be set. Specify the all-as parameter of compare-med when specifying the all-as parameter of multipath-option.
bgp4+: Number of local-as is more than maximum permitted(16)	The number of defined local-as options exceeds the maximum allowable value. Define local-as options of less than maximum 16.
bgp4+: Only External groups may be Confederation Peer	The confederation parameter is specified by the internal peer. Do not specify the confederation parameter by using the internal peer.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp4+:only one choice the gateway option or the multihop option	Both gateway option and multihop option is defined. Define a gateway option or multihop option.
bgp4+: only one choice the gateway option or the set-nexthoppeer option	Both gateway option and multihop option is defined. Define a gateway option or setnexthopper option.
bgp4+: only one choice the refresh option or the refresh-128 option	Both refresh option and refresh-128 option is defined. Define a refresh option or refresh-128 option.
bgp4+: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
bgp4+: permit-asloop may only be used with external peers	The permit-asloop option is defined for other than external peers. This option may only be used for external peers.
bgp4+: policygroup can be used in same group type	The settings of confederation parameters in the policy group are different. The settings of confederation parameters in the policy group must be the same.
bgp4+: policy-group may only be used with external groups	Policy group is specified by other than external peer. The group cannot be used by other than external peer.
bgp4+: policy-group should be used in the group declaration only	Policy group is specified by other than peer group. Specify the group as peer group option.
bgp4+: remove-private-as may only be used with external peers	The remove-private-as parameter is specified by other than the external peer. Do not specify the parameter by using the other peer than the external peer.
bgp4+: remove_private_as option must be the same in the policy group	The settings of remove-private-as parameters in the policy group are different. The settings of remove-private-as parameters in the policy group must be the same.
bgp4+: routerid not specified:BGP4+ requires it	Router ID is not defined. Specify the router ID.
bgp4+: setnexthoppeer option is not supported this group type	The setnexthoppeer option is defined in other than the internal peer. Do not specify the setnexthoppeer parameter in other than the internal peer.
bgp4+: syntax error	Syntax error
bgp4+: the BGP4+ local AS (<As1>) peer AS (<As2>) must be same for internal peers	The As number in the internal peer is different from the AS number for the own device. The AS numbers for the internal peer and routing peer must be agreed with the AS number of the own device.
	<As1>: memberAS number of local router <As2>: AS number of the counterpart device.
bgp4+: the holdtime for BGP4+ group peers (<Value>) is less than minimum permitted (3)	The hold timer value specified in a BGP4+ peer group is lower than the permitted minimum value. Define the hold timer value by 0 or 3 or more.
	<Value>: Specified hold timer
bgp4+: the holdtime for BGP4+ peer <IPv6 Prefix> (<Value>) is less than the minimum permitted (3)	The hold timer value relative to the specified peer is smaller than the allowed minimum value. Define the hold timer value by 0 or 3 or more.
	<Value>: Specified hold timer
bgp4+: the lcladdr option should be used in the group declaration only	An lcladdr parameter differs from that defined in a peer group. Do not specify the different lcladdr parameter by using the internal peer and routing peer.
bgp4+: the local as can not be used in confederation	The Local-as option is defined for other than external peers. This option may only be used for external peers.
bgp4+: the metricout option should be used in the group declaration only	The metricout parameter is different from the one specified by the peer group. Do not specify the different metricout parameter by using the internal peer and routing peer.
bgp4+: the metricout option should be used in the group declaration only in case of internal/ routing peers	The metricout parameter is different from the one specified by the peer group. Do not specify the different metricout parameter by using the internal peer and routing peer.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

bgp4+: the peer group option must be the same for policy group	The settings of peer group option in the policy group are different. The settings of peer group option in the policy group must be the same.
bgp4+: the peer option is link-local address, but the internal peeras group is not supported link-local address peering	The link local address is defined in the address of the internal peer. Define the global address or site local address in the peer address of the internal peer.
bgp4+:the refresh option must be specified with ipv6-uni	Parameters other than ipv6-uni are specified in the parameter of a refresh option. Do not specify parameters other than ipv6-uni in the parameter of a refresh option.
bgp4+:when the peer address is link-local address, gateway option must not be specified	The peer address is a link local address, but a gateway option is defined. Do not define a gateway option when a link local address is defined in the peer address.
configuration check error	Configuration information check error. If the identifiers (<id>) to be designated by the "attribute-list" command, the "network-filter" command and the "route-filter" command contain unusable characters, modify them to the correct identifiers (<id>).
dampen-flap: incorrect suppression parameters	The parameter specified in dampen-flap definition is invalid. Specify so as to meet the condition of reuse-below < suppress-above <max-flap.
dampen-flap: invalid keep-history-time value at <value> not in range 1 to 86400	The specified keep history time is invalid. Specify within the range of 1 to 86400.
	<Value>: Specified keep history time
dampen-flap: invalid max-flap value at <value> not in range 1 to 30	The specified maximum flap value is invalid. Specify within the range of 1 to 30.
	<Value>:Specified maximum flat value
dampen-flap: invalid reach-decay-time value at <value> not in range 1 to 3600	The specified reach decay time is invalid. Specify within the range of 1 to 3600.
	<Value>: Specified reach decay time
dampen-flap: invalid reuse-below value at <value> not in range 1 to 30	The specified reuse value is invalid. Specify within the range of 1 to 30.
	<Value>: Specified reuse value
dampen-flap: invalid suppress-above value at <value> not in range 1 to 30	The specified suppress value is invalid. Specify within the range of 1 to 30.
	<Value>: Specified suppress value.
dampen-flap: invalid unreach-decay-time value at <value> not in range 1 to 3600	The specified unreach decay time is invalid. Specify within the range of 1 to 3600.
	<Value>: Specified unreach decay time
dampen-flap: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
dampen-flap: syntax error	Syntax error
export: address not IPv6	Addresses other than an IPv6 prefix are specified. Specify the IPv6 prefix.
export: address should not be::	A default address is specified in an address. Specify addresses other than the local host address.export: address should not be v4-compatable.
export: address should not be v4-compat	An IPv4-compatible address is specified in an address. Specify addresses other than the IPv4-compatible address.
export: address should not be v4-mapped	An IPv4 mapped address is specified in an address. Specify addresses other than the IPv4 mapped address.
export: Attribute-filter " <Name>" cannot be specified	Filter information inherent to IPv4 is defined in IPv6. Do not specify the filter information inherent to IPv4.
	<Name>: Specified identifier

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

export: Attribute-filter not found at <Value>	The specified ID number is not defined, or cannot be found. Specify the defined ID number
	<Value>: Specified ID number
export: attribute-list name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
export: {bgp|bgp4+} attribute option of route-filter must not be define for {rip|riping|ospf_ase|ospf6_ase}	The BGP|BGP4+ attribute option for the route filter is defined against the RIP/RIPng/OSPFASE/OSPF6ASE protocol. Do not specify the BGP|BGP4+ attribute option.
export: duplicate AS path pattern in list	In export definition, an AS path pattern is duplicated. Specify a unique AS path pattern.
export: duplicate autonomous-system in list at <As>	In export definition, an AS number is duplicated. Specify a unique AS number.
	<As>: Specified As number
export: duplicate entry at <Address> mask <Mask> [exact | refine]	In export definition, a network range is duplicated. Specify a unique network range.
	<Address>: Specified Address <Mask>: Specified mask
export: duplicate gateway in list at <Address>	In export definition, a gateway address is duplicated. Specify a unique gateway address.
	<Address>: Specified gateway address
export: duplicate interface address in list at <Address>	In export definition, an interface address is duplicated. Specify a unique interface address.
	<Address>: Specified interface address
export: duplicate peer address in list at <Address>	1. In export definition, a peer address is duplicated. Specify a unique peer address.
	<Address>: Specified peer address
export: duplicate protocol specific data in list at [type <Type>] [tag <Tag>]	In export definition, an AS external-route type and tag is duplicated. Specify a unique AS external-route type and tag.
	<Type>: Specified AS external-route type <Tag>: Specified tag
export: duplicate tag in last at <Tag>	In export definition, a tag is duplicated. Specify a unique tag value.
	<Tag>: Specified tag
export: error resolving '<Host Name>': Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host Name>: Specified host name
export: gateway <IPv6 Prefix> is not global/ site-local/linklocal IPv6 address	Specified gateway is invalid. Specify the global address, site-local address or linklocal address.
	<IPv6 Prefix>: Specified gateway address
export: gateway not a host address on an attached network: <Address>	Specified gateway is not the address of the host on the connected network. Specify a gateway address on specified interface address.
	<Address>: Specified gateway address <Address>: Specified Address <Masklen>: Specified mask length
export: Interface not found at '<Interface Name>'	The specified interface name cannot be found. Specify the defined interface name.
	<Interface Name>: Specified interface name
export: Interface not found at <Address>	Interface of specified interface address is not found. Use a defined interface address.
	<Address>: Specified interface address
export: invalid attribute-list number value at <Value> not in range 1 to 65535	The specified ID number is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified ID number

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

export: invalid autonomous system value at <Value> not in range 1 to 65534	AS number is invalid. Specify a value within the range of 1 to 65534.
	<Value>: Specified AS number
export: invalid {BGP|BGP4+} {metric|localpref} metric value at <Metric> not in range 0 to 65535	In export definition, the BGP/BGP4+ metric is invalid. Specify a value within the range of 0 to 65535.
	<Metric>: Specified metric value
export: invalid domain-number value at <Domain Number> not in range 1 to 65535	OSPF or OSPFv3 domain number value is out of valid range. Specify value within the range of 1 to 65535.
	<Domain Number>: Specified domain number
export: invalid export-type value at <Value> not in range 1 to 2	AS external-route type is invalid. Use 1 or 2.
	<Value>: Specified AS external type
export: invalid external-route-tag value at <Value> not in range 0 to 2147483647	AS external-route tag value is invalid. Specify a value within the range of 0 to 2147483647.
	<Value>: Specified As external tag value.
export: invalid high end of range value at <Value> not in range 0 to {32|128}	In the between specification, upper limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.between
	<Value>: Specified upper limit value of mask
export: invalid {Inet|IPv6} mask bits value at <Value> not in range 0 to {32|128}	At masklen/prefixlen, the mask length is invalid. Specify a value within the range of 0 to 32/128.
	<Masklen>: Specified mask length
export: Invalid interface name '<Interface Name>'	The multi-home interface is specified. Do not specify multi-home interface.
	<Interface Name>: Specified interface name
export: invalid low end of range value at <Value> not in range 0 to {32|128}	In the between specification, lower limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Specified lower limit value of mask
export: invalid number of communities value at <Value> not in range 0 to 25	Specified community count is over the limit. Specify a value up to 25.
	<Value>: Specified communities value
export: invalid number of route-filter lists value at <Value> not in range 1 to 8	Specified route filter count is over the limit. Specify a value up to 8.
	<Value>: Specified communities value
export: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify within the range of 0 to 255.
	<Value>: Specified value
export: invalid { OSPF | OSPF6 } metric offset value at <Metric> not in range 1 to 16777215	The range for specifying OSPFASE/OAPF6ASE metric offset values in export definition is invalid. Specify within the range of 1 to 16777215.
	<Metric>: Specified metric offset value
export: invalid {OSPF|OSPF6} metric value at <Metric> not in range 0 to 16777215	OSPFASE/OSPF6ASE metric in the configuration information is invalid. Specify a value within the range of 0 to 16777215.
	<Metric>: Specified metric value
export: invalid policy group number value at <Group Number> not in range 1 to 16	Policy group number value is out of valid range. Specify value within the range of 1 to 16.
	<Group Number>: Specified policy group number
export: invalid range end: <Value>	In Aspath_term{m,n}, m>n or n is more than 256. Reduce start value to more than end value or assign a value less than 255 to the end value.
	<Value>: Specified end value (n)
export: invalid range start: <Value>	In aspath_term{m,n}, {m}, {m,}, m is more than 256. Specify a value less than 255.
	<Value>: Specified start value (m)
export: invalid { RIP | RIPng } metric offset value at <Metric> not in range 1 to 15	The range for specifying RIP/RIPng metric offset values in export definition is invalid. Specify within the range of 1 to 16777215.
	<Metric>: Specified metric offset value

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

export: invalid {RIP|RIPng} metric value at <Metric> not in range 1 to 16	In export definition, the RIP/RIPng metric is invalid. Specify a value within the range of 1 to 16.
	<Metric>: Specified metric value
export: invalid route-filter number value at <Value> not in range 1 to 65535	The specified ID number is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified ID number
export: invalid vpn number value at <Value> not in range 1 to <Max_Value>	The specified vpn number is invalid. Specify within the range of 1 to <Max_Value>.
	<Value>: Specified VPN number <Max_Value>Maximum VPN number
export: IPv6 Interface not found at '<Interface name>'	The interface of the specified interface name cannot be found. Specify it by using the defined interface name.
	<Interface name>: Specified interface name
export: IPv6 prefix cannot be linklocal in configuration	The link local address is specified in the network address. Do not use the link local address.
export: IPv6 prefix cannot be multicast in configuration	The multicast address is specified in the network address. Do not use the multicast address.
export: linklocal address should be followed by % (IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
export: low end of range <Mask1> shorter than prefix mask <Mask2>	In the between specification, mask range lower limit value is overlapped with specified mask. Specify the value so the mask range does not overlap with specified mask.
	<Mask1>: Specified mask range of lower limit <Mask2>: Specified mask
export: low end of range (<Value1> bits) is greater than high end (<Value2> bits) is greater	In the between specification, mask range lower limit value is greater than upper limit. Reduce lower limit value to less than upper limit value.
	<Value1>: Lower limit of Mask range <Value2>: Upper limit of Mask range
export: mask not contiguous	Bit 1 of specified mask does not continue. Use a mask where bit 1 continues.
export: metric option of route-filter must not be define for {bgp|bgp4+}	The metric option for the route filter is defined against the BGP/ BGP4+ protocol. Do not specify the metric option.
export: Non-masked bits not zero for <Address> mask <Mask>	At mask, 1 is set to non-masked bit of specified address. Set non-masked bit 0.
	<Address>: Specified address <Mask>: Specified mask
export: Non-masked bits not zero for <Address> masklen <Masklen>	At masklen, 1 is set to non-masked bit of specified address. Set non-masked bit 0.
export: not IPv6 prefix	Addresses other than an IPv6 prefix are specified. Specify the IPv6 prefix.
export: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
export: preference option of route-filter must not be define for export filter	The preference option for the route filter is defined in the export filter. Do not specify the preference option.
export: route-filter name "< Name>" cannot be specified	The specified route filter contains invalid protocol information or network information. Specify the valid route filter name.
	<Name>: Route filter name
export: route-filter name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

export: route-filter not found at <Value>	The specified ID is not defined. Specify the defined ID
	<Value>: specified ID
export: Set-attribute "<Name>" cannot be specified	Filter information inherent to IPv4 is defined in IPv6. Do not specify the filter information inherent to IPv4.
	<Name>: Specified identifier
export: Set-attribute not found at <Value>	The specified ID number is not defined, or cannot be found. Specify the defined ID number
	<Value>: Specified ID number
export: syntax error	Syntax error
export: tag option of route-filter must not be define for { bgp | bgp4+ | rip | ripng }	The tag option of a router filter is defined for an export filter or BGP/ BGP4+/RIP/RIPng protocol. Do not specify a tag option.
export: type option of route-filter must not be define for { bgp | bgp4+ | rip | ripng }	The type option for the route filter is defined against the BGP/BGP4+/ RIP/RIPng protocol. Do not specify the type option.
hosts: address should not be v4-compat	An IPv4-compatible address is specified in an address. Specify addresses other than the IPv4-compatible address.
hosts: address should not be v4-mapped	An IPv4 mapped address is specified in an address. Specify addresses other than the IPv4 mapped address.
hosts: last 64bit of IPv6 host address should not be all-zero	The lower-order 64 bits of the host address are all specified with zero. Specify the address so that all of the lower-order 64 bits are not zero.
hosts: linklocal address should be followed by % (IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
import: address not IPv6	Addresses other than an IPv6 prefix are specified. Specify the IPv6 prefix.
import: address should not be::	Default address is specified in the address. Specify addresses other than the local host address.
import: address should not be v4-compat	An IPv4-compatible address is specified in an address. Specify addresses other than the IPv4-compatible address.
import: address should not be v4-mapped	An IPv4 mapped address is specified in an address. Specify addresses other than the IPv4 mapped address.
import: Attribute-filter " <Name>" cannot be specified	Filter information inherent to IPv4 is defined in IPv6. Do not specify the filter information inherent to IPv4.
	<Name>: Specified identifier
import: Attribute-filter not found at <Value>	The specified ID number cannot be found. Specify the defined ID number
	<Value>: Specified ID number
import: attribute-list name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
import: {bgp|bgp4+} attribute option of route-filter must not be define for {rip|ripng|ospf_ase|ospf6_ase}	The BGP/BGP4+ attribute option for the route filter is defined against the RIP/RIPng/OSPFASE/OSPF6ASE protocol. Do not specify the BGP/BGP4+ attribute option.
import: duplicate AS path pattern in list	In the import definition, an AS path pattern is duplicated. Use a unique AS path pattern.
import: duplicate autonomous-system in list at <As>	In the import definition, an AS number is duplicated. Use a unique AS number.
	<As>: Specified AS number
import: duplicate entry at <Address> mask <Mask> [exact | refine]	In the import definition, a network range is duplicated. Specify a unique network range.
	import <Address>: Specified Address <Mask>: Specified Mask

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

import: duplicate gateway in list at <Address>	In the import definition, a gateway address is duplicated. Use a unique gateway address.
	<Address>: Specified gateway address
import: duplicate interface address in list at <Address>	In the import definition, an interface address is duplicated. Specify a unique interface address.
	<Address>: Specified interface address
import: duplicate peer address in list at <Peer>	Peer address is duplicated in import definition. Specify not to duplicate the peer address.
	<Peer>: Specified peer address
import: duplicate protocol specific data in list at [tag <Tag>]	In the import definition, an AS external-route type and tag is duplicated. Specify not to duplicate the tag.
	<Tag>: Specified tag value
import: error resolving '<Host Name>': Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host Name>: Specified host name
import: gateway <IPv6 Prefix> is not global/ site-local/linklocal IPv6 address	Specified gateway is invalid. Specify the global address, site-local address or linklocal address.
	<IPv6 Prefix>: Specified gateway address
import: gateway not a host address on an attached network: <Address>	Specified gateway is not the address of the host on the connected network. Specify a gateway address on the specified interface address.
	<Address>: Specified gateway address <Value>: Upper limit of specified mask range
import: Interface not found at '<Interface Name>'	The specified interface name cannot be found. Specify the defined interface name.
import: Interface not found at <Address>	Interface of specified interface address is not found. Use a defined interface address.
	<Address>: Specified interface address
import: invalid attribute-list number value at <Value> not in range 1 to 65535	The specified ID number is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified ID number
import: invalid autonomous system value at <Value> not in range 1 to 65534	AS number is invalid. Specify a value within the range of 1 to 65534.
	<Value>: Specified AS number
import: invalid domain-number value at <Domain Number> not in range 1 to 65535	OSPF domain number value is out of valid range. Specify value within the range of 1 to 65535.
	<Domain Number>: Specified domain-number
import: invalid external-route-tag value at <Value> not in range 0 to 2147483647	AS external-route-tag value is invalid. Specify a value within the range of 0 to 2147483647.
	<Value>: Specified AS external-route-tag value
import: invalid high end of range value at <Value> not in range 0 to {32|128}	<In the between specification, upper limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
import: invalid {inet|IPv6} mask bits value at <Masklen> not in range 0 to {32|128}	At masklen/prefix, the mask length is invalid. Specify a value within the range of 0 to 32/128.
	<Masklen>: Specified Mask length
import: Invalid interface name '<Interface Name>'	The multi-home interface is specified. Do not specify multi-home interface.
	<Interface Name>: Specified interface name
import: invalid low end of range value at <Value> not in range 0 to {32|128}	In the between specification, lower limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Specified lower limit of specified mask range
import: invalid number of communities value at <Value> not in range 0 to 25	Specified community count is over the limit. Specify the count up to 25.
	<Value>: Specified community count

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

import: invalid number of route-filter lists value at <Value> not in range 1 to 8	Specified route filter count is over the limit. Specify the count up to 8.
	<Value>: Specified route filter count
import: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
import: invalid preference value at <Value> not in range 2 to 255	Preference value is invalid. Specify a value within the range of 2 to 255.
	<Value>: Specified preference value
import: invalid policy group number value at <Group Number> not in range 1 to 16	Policy group number value is out of valid range. Specify value within the range of 1 to 16.
	<Group Number>: Specified policy group number
import: invalid range end: <Value>	In aspath_term{m,n}, m>n or n is more than 256. Set a start value less than the end value or assign a value less than 255 to the end value.
	<Value>: Specified end value (n)
import: invalid range start: <Value>	In aspath_term {m, n}, {m}, {m,}, more than 256 is specified for m. Use a value less than 255.
	<Value>: Specified start value (m)
import: invalid route-filter number value at <Value> not in range 1 to 65535	ID number is out of valid range. Specify value within the range of 1 to 65535.
	<Value>: Specified ID number
import invalid vpn number value at <Value> not in range 1 to <Max_Value>	VPN number is out of valid range. Specify a value within the range of 1 to <Max_Value>.
	<Value>: Specified VPN number <Max_Value>Maximum VPN number
import: IPv6 Interface not found at '<Interface name>'	The interface of the specified interface name cannot be found. Specify it by using the defined interface name.
	<Interface name>: Specified interface name
import: IPv6 prefix cannot be linklocal in configuration	The link local address is specified in the network address. Do not use the link local address.
import: IPv6 prefix cannot be multicast in configuration	The multicast address is specified in the network address. Do not use the multicast address.
import: linklocal address should be followed by %(IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
import: low end of range (<Value1> bits) is greater than high end (<Value2> bits)	In the between specification, lower limit of the mask range is greater than upper limit.Reduce lower limit value of the mask range to less than upper limit value.
	<Value1>: Lower limit of mask range <Value2>: Upper limit of mask range
import: low end of range <Mask1> shorter than prefix mask <Mask2>	In the between specification, lower limit of the mask range is overlapped with specified mask. Correct the value so the mask range does not overlap with specified mask.
	<Mask1>: Lower limit of specified risk range <Mask2>: Specified mask
import: mask not contiguous	Bit 1 of the specified mask does not continue. Use a mask where bit 1 continues.
import: metric option of route-filter must not be define for {import filter | bgp | bgp4+}	The metric option for the route filter is defined in the import filter or the BGP/BGP4+ protocol. Do not specify the metric option.
import: Non-masked bits not zero for <Address> mask <Mask>	At mask, 1 is set to non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Mask>: Specified mask

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

import: Non-masked bits not zero for <Address> masklen <Masklen>	At masklen, 1 is set to non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Masklen>: Specified mask length
import: not IPv6 prefix	Addresses other than an IPv6 prefix are specified. Specify the IPv6 prefix.
import: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
import: proto option of route-filter must not be define for import filter	The proto option for the route filter is defined in the import filter. Do not specify the proto option.
import: route-filter name "<Name>" cannot be specified	The specified route filter contains invalid protocol information or network information. Specify the valid route filter name.
import: route-filter name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
import: route-filter not found at <Value>	The specified ID is not defined Specify a defined ID.
	<Value>: Specified ID
import: Set-attribute "<Name>" cannot be specified	Filter information inherent to IPv4 is defined in IPv6. Do not specify the filter information inherent to IPv4.
	<Name>: Specified identifier
import: Set-attribute not found at <Value>	The specified ID number cannot be found. Specify the defined ID number
	<Value>: Specified ID number
import: syntax error	Syntax error
import: tag option of route-filter must not be define for {import filter | bgp | bgp4+ | rip | ripng}	The tag option for the route filter is defined in the import filter or the BGP/BGP4+/RIP/RIPng protocol. Do not specify the tag option.
import: tag option of route-filter must not be define for {import filter | bgp | bgp4+ | rip | ripng}	The tag option for the route filter is defined in the import filter or the BGP/BGP4+/RIP/RIPng. Do not specify the tag option.
ip: invalid vpn number value at <Value> not in range 1 to <Max_Value>	VPN number is out of valid range. Specify value within the range of 1 to <Max_Value>.
	<Value>: Specified VPN number <Max_Value>Maximum VPN number
network-filter: duplicate entry at <Address> mask <Mask> [exact | refine]	In the network-filter definition, an network range is duplicated. Specify a unique network range
	<Address>: Specified Address <Mask>: Specified mask
network-filter: duplicate entry at <Prefix>/ <Prefixlen> [exact | refine]	The network range is defined in duplication in the network-filter definition. Specify the range so that the network range will not be duplicated.
	<Prefix>: Specified prefix <Prefixlen> Specified prefix length
network-filter: duplicate network-filter at <Value>	The specified ID has been already registered. Specify the other ID.
	<Value>: Specified ID
network-filter: each network must belong to the same family: <Name>	A network information of different address family is mixed in the network-filter. Specify the information so does not overlap with deferent address in one network-filter name.
	<Value>: Network filter name
network-filter: invalid high end of range value at <Value> not in range 0 to {32|128}	In the between specification, upper limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Upper limit of specified mask range

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

network-filter: invalid {inet|IPv6} mask bits value at <Masklen> not in range 0 to {32|128}	At masklen/prefixlen. the mask length is valid. Specify value within the range of 0 to 32/128.
	<Masklen>: Specified mask length
network-filter: invalid low end of range value at <Value> not in range 0 to {32|128}	In the between specification, lower limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Lower limit of specified mask range
network-filter: invalid network-filter number value at <Value> not in range 1 to 65535.	ID number is out of valid range. Specify value within the range of 1 to 65535.
	<Value>: Specified ID number
network-filter: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
network-filter: IPv6 prefix cannot be linklocal in configuration	The link local address is specified in the network address. Do not use the link local address.
network-filter: IPv6 prefix cannot be multicast in configuration	The multicast address is specified in the network address. Do not use the multicast address.
network-filter: linklocal address should be followed by %(IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
network-filter: low end of range (<Value1> bits) is greater than high end (<Value2> bits)	In the between specification, lower limit of the mask range is greater than upper limit. Reduce lower limit value of the mask range to less than upper limit value.
	<Value1>: Lower limit of mask range <Value2>: Upper limit of mask range
network-filter: low end of range <Mask1> shorter than prefix mask <Mask2>	In the between specification, lower limit of mask range is overlapped. Correct the value so the mask range does not overlap with specified mask.
	<Mask1>: Lower limit of specified mask range <Mask2>: Specified mask
network-filter: mask not contiguous	Bit 1 of the specified mask does not continue. Use a mask where bit 1 continues.
network-filter: network-filter name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
network-filter: Non-masked bits not zero for <Address> mask <Mask>	At mask, 1 is set to non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Mask>: Specified mask
network-filter: Non-masked bits not zero for <Address> masklen <Masklen>	At masklen, 1 is set to non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Masklen>: Specified mask length
network-filter: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
network-filter: syntax error	Syntax error
options: error resolving '<Host Name>': Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host Name>: Specified host name
options: gen-prefix-route option can be specified only with the composition with the same network of the both ends of an point-to-point interface.	A gen-prefix-route option cannot be specified when an interface in which the network of local and remote addresses differs exists in a point-to-point interface. Make identical the network of the local and remote addresses in a point-to-point interface when specifying a gen-prefix-route option.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

options: invalid maximum paths value at <Value> not in range 1 to 16	The specified maximum path count in options definition is invalid. Specify in the range of 1 to 16.
	<Value>: Specified maximum path count
options: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
options: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
options: syntax error	Syntax error
ospf: 2 or more areas have been defined: need to configure backbone	Although two or more OSPF areas have been defined, a backbone area has not been defined. Define a backbone area.
ospf: authentication-key "<Key>" <Length> longer than [8 | 16] characters	Specified authentication key is longer than 8 characters (for simple) or16 characters (for md5). For simple, the length is up to 8 characters (or hexadecimal 16 digits). For md5, the length is up to 16 characters (or hexadecimal 32 digits).
	<Key>: Specified authentication key <Length>: Specified authentication key length
ospf: authentication-key longer than [8 | 16] characters	Specified authentication key is longer than 8 characters (for simple) or 16 characters (for md5). For simple, the length is up to 8 characters (or hexadecimal 16 digits). For md5, the length is up to 16 characters (or hexadecimal 32 digits).
ospf: day must be between 1 and 31	Specified date is invalid. Specify a value within the range of 1 to 31.
ospf: domain <Domain Number> duplicated	OSPF domain number is duplicated. Do not define in duplication.
	<Domain Number>: Specified domain number
ospf: duplicate area	OSPF area ID is duplicated. Use a unique area ID.
ospf: duplicate entry at <Address> mask <Mask> [exact | refine]	Network range is duplicated in the ospf definition. Use a unique network range.
	<Address>: Specified address <Mask>: Specified mask
ospf: duplicate interface address in list at <Address>	Interface address is duplicated in the ospf definition. Use a unique interface address.
	<Address>: Specified interface address
ospf: duplicate ospf clause	OSPF definition is duplicated. Delete one of the two
ospf: duplicate ospf interface parameter - “cost”	Interface parameter “cost” is duplicated in OSPF definition. Do not duplicate an interface cost.
ospf: duplicate ospf interface parameter - "nonbroadcast"	Interface type is duplicated in OSPF area definition. Do not duplicate interface type.
ospf: duplicate virtual link	In the virtual link definition of ospf, the group of a passage area and adjacent router ID has been already defined. Specify the group of an identical passage area and adjacent router ID so that they are not duplicated.
ospf: error in common options -- possible duplicate or conflicting option?	In the OSPF area definition, an interface option is duplicated. Do not duplicate an interface option.
ospf: error resolving ’<Host Name>’: Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host Name>: Specified host name
ospf: gateway not a host address on an attached network: <Address>	Specified gateway is not address of host on connected network. Specify a gateway address on specified interface address.
	<Address>: Specified gateway address
ospf: hour must be between 0 and 23	Specified time (hour) is invalid. Specify a value within the range of 0 to 23.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

ospf: Interface not found at '<Interface Name>'	The specified interface name cannot be found. Specify the defined interface name.
	<Interface Name>: Specified interface name
ospf: Interface not found at <address>	Interface of specified interface address is not found. Use defined interface address.
	<Address>: Specified interface address
ospf: invalid area-number value at <Value> not in range 0 to 4294967295	<value> not in range 0 to 4294967295 Specified OSPF area ID value is invalid. Specify a value within the range of 0.0.0.1-255.255.255.255.
	<Value>: Specified area ID
ospf: Invalid domain configuration value at '5' not in range 0 to 4	The number of configuration definitions of OSPF Domain exceeds the maximum of 4. Delete one of the configuration definitions of OSPF Domain.
ospf: invalid domain-number value at <Domain Number> not in range 1 to 65535 OSPF domain number is out of valid range.	Specify value within the range of 1 to 65535.
	<Domain Number>: Specified domain number
ospf: invalid export-type value at <Value> not in range 1 to 2	Specified AS external-route type value is invalid. Use 1 or 2.
	<Value>: Specified AS external-type
ospf: invalid external-route-tag value at <Value> not in range 0 to 2147483647	Specified AS external-route tag value is invalid. Specify a value within the range of 0 to 2147483647.
	<Value>: Specified AS external-route tag value
ospf: invalid hello-interval value at <Value> not in range 0 to 255	In the OSPF definition, the hello-interval value is out of valid range. Specify a value within the range of 0 to 255.
	<Value>: Specified hello-interval value
ospf: invalid inet mask bits value at <Masklen> not in range 0 to 32	In masklen, the specified mask length is invalid. Use a value within the range of 0 to 32.
	<Masklen>: Specified mask length
ospf: Invalid interface name '<Interface Name>'	The multi-home interface is specified. Do not specify multi-home interface.
	<Interface Name>: Specified interface name
ospf: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
ospf: invalid OSPF cost value at <Cost> not in range 0 to 65535	OSPF cost value in the following configuration information is invalid. Use a value within the range of 0 to 65535.
	<Cost>: Specified cost value.
ospf: invalid OSPF interface cost value at <Cost> not in range 1 to 65535	OSPF interface cost value in the following configuration information is invalid. Use a value within the range of 1 to 65535.
	<Cost>: Specified interface cost value.
ospf: invalid poll-interval value at <Value> not in range 0 to 255	In the OSPF definition, the poll-interval value is out of valid range. Specify a value within the range of 0 to 255.
	<Value>: Specified poll-interval value
ospf: invalid preference value at <Value> not in range 2 to 255	Specified preference value is invalid. Specify a value within the range of 0 to 255.
	<Value>: Specified preference value
ospf: invalid priority value at <Value> not in range 0 to 255	In the OSPF definition, specified priority value is invalid. Specify a value within the range of 0 to 255.
	<Value>: Specified priority value
ospf: invalid range <Address>/<Mask>	In the OSPF definition, specified network value is invalid (0.0.0.0). Use a value other than 0.0.0.0.
	<Address>: Specified address <Mask>: Specified mask

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

ospf: invalid retransmit-interval value at <Value> not in range 1 to 65535	In the OSPF area definition, the retransmit-interval value is out of the valid range. Specify a value within the range of 1 to 65535.
	<Value>: Specified retransmit-interval value
ospf: invalid router-dead-interval value at <Value> not in range 1 to 65535	In the OSPF definition, the router-dead-interval value is out of valid range. Specify a value within the range of 1 to 65535.
	<Value>: Specified router-dead-interval value
ospf: invalid seconds value at <Value> not in range 0 to 4294967295	Specified timer value is invalid. Specify a value within the range of 0 to 4294967295.
	<Value>: Specified timer value
ospf: invalid transit-delay value at <Value> not in range 1 to 65535	In the OSPF definition, the transit-delay value is out of valid range. Specify a value within the range of 1 to 65535.
	<Value>: Specified transit-delay value
ospf: invalid vpn number value at <Value> not in range 1 to <Max_Value>	The range of VPN value is invalid. Specify a value within the range of 1 to <Max_Value>.
	<Value>: Specified VPN number <Max_Value>: Maximum VPN number
ospf: key id must be between 0 and 255	Specified MD5 authentication key ID is invalid. Specify a value within the range of 0 to 255.
ospf: keys cannot have same start time	MD5 authentication message digest generation start time is duplicated. Do not duplicate the start time.
ospf: mask not contiguous	Bit 1 of the specified mask does not continue. Use a mask where bit 1 continues.
ospf: minute must be between 0 and 59	Specified time (minute) is invalid. Specify a value within the range of 0 to 59.
ospf: month must be between 1 and 12	Specified month is invalid. Specify a value within the range of 1 to 12.
ospf: multipath option not valid for vpn route	The Multipath option is defined for VPN. VPN does not support multipath option.
ospf: neighbor-id must be an IP address	The IP address defined to neighborhood is invalid. Specify in IP address format.
ospf: net range already specified	Network parameter is already specified in OSPF area definition. Do not duplicate a networks parameter.
ospf: Non-masked bits not zero for <Address> masklen <Masklen>	In masklen, 1 is specified for non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Masklen>: Specified mask length
ospf: Non-masked bits not zero for <Address> mask <Mask>	In mask, 1 is specified for non-masked bit of specified address. Specify 0 to non-masked bit 0.
	<Address>: Specified Address <Mask>: Specified mask
ospf: nssa option not valid for backbone	Nssa option is defined in a backbone area. Do not defined a nssa option in a backbone area.
ospf: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
ospf: Router ID not defined	Router ID is not defined. Specify the Router ID.
ospf: secondary auth was overwritten by md5 for virtual link to <Neighbor ID> in Domain <Domain ID> [on VPN <VPN ID>].	In a specified virtual link, both MD5 authentication and the 2nd authentication key are defined. Delete the unnecessary authentication method.
	<Neighbor ID>: router ID of the adjacent OSPF virtual link router <Domain ID>: specified domain No. of the OSPF virtual link <VPN ID>: specified VPN No. of the OSPF virtual link.
ospf: stop accept time must be later than start accept time	MD5 authentication message digest accept end time is earlier than start time. Set the value so start time is earlier than end time.

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

ospf: stop generate time must be later than start generate time	MD5 authentication message digest generation end time is earlier than start time. Set the value so start time is earlier than end time.
ospf: stub option not valid for backbone	Stub parameter is specified in the OSPF backbone definition. Do not specify a stub parameter in a backbone area.
ospf: syntax error	Syntax error
ospf: this Router ID and Neighbor ID must be different	This Router ID and Neighbor ID are the same. Specify the different IDs to this Router and Neighbor.
ospf: transit-area can not be the 'backbone'area	The transit area of virtual link is defined outside the backbone area. Set virtual link other than backbone area.
ospf: unknown authentication type: <Value>	In the OSPF definition, authentication type is illegal. For authentication type, specify "simple" or "md5."
	<Value>: Specified authentication type
ospf: virtual links only allowed in 'backbone'area	The virtual link is defined outside the backbone area. Set virtual link within backbone area.
ospf: year must be after 1970	The year is before 1970. Specify a year after 1970.
ospf6: 2 or more areas have been defined: need to configure backbone	Two or more OSPFv3 areas are defined, but a backbone area is not defined. Define a backbone area.
ospf6: domain <Domain Number> duplicated	he OSPFv3 domain number is duplicate-defined. Do not duplicate-define the OSPFv3 domain number.
ospf6: duplicate area	The area ID of OSPFv3 is duplicated for definition. Specify area ID so that it is not duplicated.
ospf6: duplicate entry at <Prefix>/<Prefixlen>	The network range is defined in duplication in the OSPVv3 definition. Specify the range so that the network range will not be duplicated.
	<Prefix>: Specified prefix <Prefixlen> Specified prefix length
ospf6: duplicate ospf interface parameter -- "cost"	In the area definition of OSPFv3, the interface cost of an interface parameter is double-defined. Do not double-define an interface cost.
ospf6: duplicate ospf6 clause	OSPFv3 is double-defined. Delete one of the definitions.
ospf6: duplicate virtual link	The pair of the passage area and the adjacent router ID has already been defined in the hypothetical link definition of the OSPFv3. Specify the pair so that the pair of the passage area and the adjacent router ID will not be duplicated.
ospf6: error in common options --possible duplicate or conflicting option?	In the area definition of OSPFv3, the interface cost of an interface parameter is double-defined. Do not double-define an interface option.
ospf6: Interface not found at ' <Interface Name>'	The interface of the specified interface name cannot be found. Specify it by using the defined interface name.
	<Interface Name>: Specified interface name
ospf6: invalid area-number value at '<Value>' not in range 1 to 4294967295	OSPFv3 area ID is invalid. Specify within the range of 0.0.0.1 to 255.255.255.255.
	<Value>: Specified area ID
ospf6: Invalid domain configuration value at '5' not in range 0 to 4	The number of OSPFv3 domain configuration definitions exceeds four upper-limit values. Delete any of the OSPFv3 domain configuration definitions.
ospf6: invalid domain-number value at <Domain Number> not in range 1 to 65535	The OSPFv3 domain number is invalid. Specify within the range of 1 to 65535.
	<Domain Number>: Specified domain number
ospf6: invalid export-type value at '<Value>' not in range 1 to 2	The AS external type is invalid. Specify within the range of 1 to 2.
	<Value>: Specified AS external route type
ospf6: invalid external-route-tag value at <Value> not in range 0 to 2147483647	The AS external tag value is invalid. Specify within the range of 1 to 2147483647.
	<Value>: Specified AS external tag value

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

ospf6: invalid hello-interval value at '<Value>' not in range 1 to 255	The hello-interval of OSPFv3 interface parameter is invalid. Specify within the range of 1 to 255.
	<Value>: Specified hello-interval value
ospf6: invalid instance value at '<Value>' not in range 0 to 255	The OSPFv3 interface parameter instance is invalid. Specify within the range of 0 to 255.
	<Value>: Specified instance value
ospf6: invalid octet value at '<Value>' not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
ospf6: invalid OSPF6 cost value at '<Cost>' not in range 0 to 65535	The OSPFv3 cost in configuration information is invalid. Specify within the range of 0 to 65535.
	<Cost>: Specified cost value
ospf6: invalid OSPF6 interface cost value at <Cost> not in range 1 to 65535	The OSPFv3 interface cost in configuration information is invalid. Specify within the range of 1to 65535.
	<Cost>: Specified interface cost value
ospf6: invalid preference value at <Value> not in range 2 to 255	The preference value is invalid. Specify within the range of 2 to 255.
	<Value>: Specified preference value
ospf6: invalid priority value at '<Value>' not in range 0 to 255	The OSPFv3 interface parameter priority is invalid. Specify within the range of 0 to 255.
	<Value>: Specified priority value
ospf6: invalid range <Prefix>/ <Prefixlen>	Incorrect (::/0) value was specified in the network range in the area definition of the OSPFv3. Specify the value in other than ::/0.
	<Prefix>: Specified prefix <Prefixlen>: Specified prefix length
ospf6: invalid retransmit-interval value at '<Value>' not in range 1 to 65535	The interface parameter retransmit-interval in OSPFv3 area definition is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified retransmit-interval value
ospf6: invalid router-dead-interval value at '<Value>' not in range 1 to 65535	OSPFv3 interface parameter router-dead-interval is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified router-dead-interval value
ospf6: invalid transit-delay value at '<Value>' not in range 1 to 65535	OSPFv3 interface parameter transit-delay is invalid. Specify within the range of 1 to 65535.
	<Value>: Specified transit-delay value
ospf6: neighbor-id must be an IP address	The IP address defined in the neighborhood is incorrect. Specify it in the IP address form.
ospf6: net range already specified	In the area definition of OSPFv3, the interface cost of an networks parameter is double-defined. Do not double-define an networks parameter.
ospf6: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
ospf6: Router ID not defined	Router ID is not defined. Specify the Router ID.
ospf6: stub option not valid for backbone	Stub parameter is defined in the OSPVv3 definition. Does not specify stub parameter in backbone area.
ospf6: syntax error	Syntax error
ospf6: this Router ID and Neighbor ID must be different	The local router ID must be different from the adjacent router ID of a virtual link.
ospf6: transit-area can not be the 'backbone' area	The passage area of a virtual link is defined in a backbone area. Define the passage area in areas other than the backbone area.
ospf6: virtual links only allowed in 'backbone' area	The hypothetical link is defined in an area other than the backbone area. Define it in the backbone area.
rip: duplicate interface address in list at <Address>	Interface address definition is duplicated in rip. Use a unique interface address.
	<Address>: Specified interface address

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

rip: duplicate rip clause	The rip definition is duplicated. Delete one of the two.
rip: duplicate rip interface parameter	Interface parameter of rip is duplicated. Use a unique interface parameter.
rip: Interface not found at '<Interface Name>'	Specified interface cannot be found. Specify the defined interface name.
	<Interface Name>: Specified interface name
rip: Interface not found at <Address>	Interface of the specified interface address is not found. Use defined interface address.
	<Address>: Specified interface address
rip: invalid aging time value at '<Time>' not in range 1 to 360	The specified engine timer value is invalid. Specify within the range of 1 to 360.
	<Time>: Specified timer value
rip: invalid holdcount value at '<Count>' not in range 1 to 8	The specified hold down count is invalid. Specify within the range of 1 to 8.
	<Count>: Specified hold down count
rip: Invalid interface name '<Interface Name>'	The multi-home interface is specified. Do not define multi-home interface.
	<Interface Name>: Specified interface name
rip: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
rip: invalid preference value at <Value> not in range 2 to 255	Preference value is out of valid range. Use a value within the range of 2 to 255.
	<Value>: Specified preference value
rip: invalid RIP metric value at <Metric> not in range 1 to 16	RIP metric specification range is illegal. Specify value within the range of 1 to 16.
	<Metric>: Specified metric value
rip: invalid RIP metricin value at <Metric> not in range 0 to 16	RIP metric specification range is illegal. Specify value within the range of 0 to 16.
	<Metric>: Specified metric value
rip: invalid update time value at '<Time>' not in range 1 to 60	The specified update time is invalid. Specify within the range of 1 to 60.
	<Time>: Specified timer value
rip: invalid version	Illegal version number is specified as the version parameter of rip. Use 1 or 2.
rip: invalid vpn number value at <Value> not in range 1 to <Max_Value>	Vpn specification range is invalid. Specify within the range of 1 to <Max_Value>.
	<Value>: Specified vpn number <Max_Value>Maximum VPN number
rip: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
rip: options not valid with version 1	Broadcast/multicast parameter specified in version 1 of rip. Do not specify a broadcast/multicast parameter in rip-1.
rip: syntax error	Syntax error
ripng: duplicate interface address in list	In the ripng definition, an interface address is duplicated. Specify a unique interface address.
	<IPv6 Prefix>: Specified Gateway Address
ripng: error resolving '<IPv6 Prefix>': Unknown host	The specified host name is not found. Specify a defined host name.
	<Host Name>: Specified host name

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

ripng: invalid aging time value at '<Time>' not in range 1 to 360	The specified aging timer value is invalid. Specify within the range of 1 to 360.
	<Time>: Specified timer value
ripng: invalid external-route-tag value at '<Value>' not in range 1 to 65535	Range of specifying the tag value for AS external route is incorrect. Specify in the range of 0 to 65535
	<Value>: Specified AS external route type.
ripng: invalid holdcount value at '<Count>' not in range 1 to 8	The specified hold down count is invalid. Specify within the range of 1 to 8.
	<Count>: Specified hold down count
ripng: invalid preference value at '<Value>' not in range 2 to 255	Range of specifying the preference value is incorrect. Specify in the range of 2 to 255.
	<Value>: Specified preference value
ripng: invalid RIPng metric value at '<Metric>' not in range 1 to 16	RIPng metric specification range is illegal. Specify value within the range of 1 to 16.
	<Metric>: Specified metric value
ripng: invalid update time value at '<Time>' not in range 1 to 60	The specified update time is invalid. Specify within the range of 1 to 60.
	<Time>: Specified timer value
ripng: IPv6 Interface not found at '<Interface name>'	The specified interface name cannot be found. Specify the defined interface name.
	<Interface Name>: Specified interface name
ripng: IPv6 Interface should be specified by its name	Specify it by using the defined interface name.
ripng: parse_proto_seen: duplicate ripng clause	The RIPng definition is duplicated. Delete one of the two.
ripng: syntax error	Syntax error
route-filter: address should not be::	Default address is specified in the address. Specify addresses other than the local host address.
route-filter: address should not be v4-compat	An IPv4-compatible address is specified in an address. Specify addresses other than the IPv4-compatible address.
route-filter: address should not be v4-mapped	An IPv4 mapped address is specified in an address. Specify addresses other than the IPv4 mapped address.
route-filter: Attribute-filter not found at <Value>	The specified ID number is not defined Specify a defined ID number.
	<Value>: Specified ID number
route-filter: attribute-list name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
route-filter: duplicate entry at <Address> mask <Mask> [exact | refine] mask <Mask>	In the route-filter definition, an network range is duplicated. Specify a unique network range.
	<Address>: Specified Address <Mask>: Specified Mask
route-filter: duplicate entry at <Prefix>/ <Prefixlen> [exact | refine]	In the route-filter definition, an network range is duplicated. Specify a unique network range.
	<Prefix>>: Specified prefix <Prefixlen>: Specified prefix length
route-filter: duplicate autonomous-system in list at '<As>'	In the route-filter definition, an AS number is duplicated. Specify a unique AS number.
	<As>: Specified AS number
route-filter: duplicate extended community	An extended community is duplicated. Specify a unique extended community.
route-filter: duplicate interface in list at '<Interface Name>'	In the route-filter definition, an interface name is duplicated. Specify a unique interface name.
	<Interface Name>: Specified Gateway Address

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

route-filter: duplicate interface address in list	In the route-filter definition, an interface address is duplicated. Specify a unique interface address.
	<IPv6 Prefix>: Specified Gateway Address
route-filter: duplicate peer address in list at '<Peer>	In the route-filter definition, a peer address is duplicated. Specify a unique peer address.
	<Peer>: Specified peer address
route-filter: duplicate proto in list at '<Protocol>'	In the route-filter definition, a protocol is duplicated. Specify a unique protocol.
	< Protocol >: Specified protocol
route-filter: duplicate route-filter at <Value>	The specified ID has been already registered. Specify the other ID.
	<Value>: Specified ID
route-filter: duplicate tag in list at '<Tag>'	In the route-filter definition, a tag is duplicated. Specify a unique tag.
	< tag >: Specified tag value
route-filter: error resolving '<Host Name>': Unknown host	The specified host name is not found. Specify a defined host name.
	<Host Name>: Specified host name
route-filter: gateway <IPv6 Prefix> is not global/site-local/ linklocal IPv6 address	Specified gateway address is invalid. Specify global/site-local/ linklocal address.
	<IPv6 Prefix>: Specified gateway address
route-filter: gateway not a host address on an attached network : <Address>	Specified gateway is not the address of the host on the connected network. Specify a gateway address on the specified interface address.
	<Address>: Specified gateway address
route-filter: Interface not found at '<Interface Name>'	The specified interface name cannot be found. Specify the defined interface name.
	<Interface Name>: Specified interface name
route-filter: Interface not found at <Address>	Interface of specified interface address is not found. Use a defined interface address.
	<Address>: Specified interface address
route-filter: invalid as_count value at <Value> not in range 1 to 25	Ascount value is out of valid range. Specify value within the range of 1 to 25.
	<Value>: Specified ascount value
route-filter: invalid attribute-list number value at <Value> not in range 1 to 65535	ID number is out of valid range. Specify value within the range of 1 to 65535.
	<Value>: Specified ID number
route-filter: invalid autonomous system number value at <Value> not in range 1 to 65534	Specified range of AS number in extended community is invalid. Specify in the range of 1 to 65534.
	<Value>: Specified AS number
route-filter: invalid autonomous system value at <Value> not in range 1 to 65534	AS number is invalid. Specify a value within the range of 1 to 65534.
	<Value>: Specified AS number
route-filter: invalid {BGP|BGP4+} metric offset value at <Metric> not in range 1 to 4294967295	Specified MED offset value is out of valid range. Specify value within the range of 1 to 4294967295.
	<Metric>: Specified MED offset value.
route-filter: invalid BGP metric value at <Metric> not in range 0 to 65535	Specified MED value is out of valid range. Specify value within the range of 0 to 65535.
	<Metric>: Specified MED value
route-filter: invalid export-type value at <Value> not in range 1 to 2	Range of specifying the AS external route type is incorrect. Specify by using 1 or 2. <Value>: Specified AS external route type.
	<Value>: Specified AS external route type
route-filter: invalid external-route-tag value at <Value> not in range 0 to 2147483647.	Range of specifying the tag value for AS external route is incorrect. Specify in the range of 0 to 2147483647.
	<Value>: Specified As external route tag value

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

route-filter: invalid domain-number value at <Domain Number> not in range 1 to 65535.	OSPF or OSPFv3 domain number is out of valid range. Specify a value within the range of 1 to 65535.
	<Domain Number>: Specified domain number
route-filter: invalid high end of range value at <Value> not in range 0 to {32|128}	In the between specification, upper limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Upper limit of Specified Mask range
route-filter: invalid index number in extended community number value at <Value> not in range 0 to { 65535 | 4294967295 }	Specified range of ID number in extended community is invalid. Specify in the range of 0 to 65534 /4294967295.
	<Value>: Specified ID number
route-filter: invalid {inet|IPv6} mask bits value at <Value> not in range 0 to {32|128}	At masklen/prefixlen, the mask length is valid. Specify value within the range of 0 to 32/128.
	<Masklen>: Specified mask length
route-filter: Invalid interface name '<Interface Name>'	The multi-home interface is specified. Do not specify multi-home interface.
	<Interface Name>: Specified interface name
route-filter: invalid localpref value at <Localpref> not in range 0 to 65535	Specified LOCALPREF value is out of valid range. Specify value within the range of 0 to 65535.
	<Localpref>: Specified LOCALPREF value.
route-filter: invalid localpref offset value at <Localpref> not in range 1 to 65535	Specified LOCALPREF offset value is out of valid range. Specify value within the range of +1 to +65535 or -1 to -65535.
	<Localpref>: Specified LOCALPREF offset value.
route-filter: invalid low end of range value at <Value> not in range 0 to {32|128}	In the between specification, lower limit value of mask range is invalid. Specify a value within the range of 0 to 32/128.
	<Value>: Lower limit of specified mask range value
route-filter: invalid network-filter number value at <Value> not in range 1 to 65535	ID number is out of valid range. Specify value within the range of 1 to 65535.
	<Value>: Specified ID number
route-filter: invalid number of communities value at <Value> not in range 0 to 25	Specified community count is over the limit. Specify a value up to 25.
	<Value>: Specified community count
route-filter: invalid number of extended communities value at <Value> not in range 1 to 25	The number of extended communities to be defined exceeds the maximum number of extended communities to be defined. Specify a value of 25 or less.
	<Value>: Extended community number
route-filter: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
route-filter: invalid policy group number value at <Group Number> not in range 1 to 16	Policy group number is out of valid range. Specify a value within the range of 1 to 16.
	<Group Number>: Specified mask length
route-filter: invalid preference value at <Value> not in range 2 to 255	Range of specifying the preference value is incorrect. Specify in the range of 2 to 255.
	<Value>: Specified preference value
route-filter: invalid range end: <Value>	In Aspath_term {m, n}, m>n or n is 0. Specify start value less than end value or assign a value other than 0 to the end value.
	<Value>: Specified end value(n)
route-filter: invalid range start: <Value>	In aspath_term {m, n}, {m}, {m,}, m is 0. Specify a value other than 0.
	<Value>: Specified start value (m)
route-filter: invalid route-filter number value at <Value> not in range 1 to 65535 value	ID number is out of valid range. Specify value within the range of 1 to 65535.
	<Value>: Specified ID number
route-filter: invalid route-filter sequence number value at <Value> not in range 1 to 65535	Sequence number is out of valid range. Specify value within the range of 1 to 65535.
	<Value>: Specified sequence number

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

route-filter: invalid vpn number value at <Value> not in range 1 to <Max_Value>	Vpn number specification range is invalid. Specify value within the range of 1 to <Max_Value>.
	<Value>: Specified vpn number <Max_Value>Maximum VPN number
route-filter: ipv4 protocol and ipv6 protocol must not be intermingled: <Name>	ipv4 routing protocol information exists together with ipv6 routing protocol information. Specify the two information items so that they do not coexist in one route filter name.
	<Name>: Route filter name
route-filter: IPv6 prefix cannot be linklocal in configuration	The link local address is specified in the network address. Do not use the link local address.
route-filter: IPv6 prefix cannot be multicast in configuration	The multicast address is specified in the network address. Do not use the multicast address.
route-filter: linklocal address should be followed by %(IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
route-filter: low end of range <Mask1> shorter than prefix mask <Mask2>	In the between specification, lower limit of the mask range is overlapped with specified mask. Correct the value so the mask range does not overlap with specified mask.
	<Mask1>: Lower limit of specified mask range <Mask2>: Specified mask
route-filter: low end of range (<Value1> bits) is greater than high end (<Value2> bits)	In the between specification, lower limit of the mask range is greater than upper limit. Reduce lower limit value of the mask range to less than upper limit value.
	<Value1>: Lower limit of mask range <Value2>: Upper limit of mask range
route-filter: mask not contiguous	Bit 1 of the specified mask does not continue. Use a mask where bit 1 continues.
route-filter: network-filter name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: Specified ID
route-filter: network-filter not found at <Value>	The specified ID number is not defined. Specify a defined ID number
	<Value>: specified ID number
route-filter: Non-masked bits not zero for <Address> mask <Mask>	At mask, 1 is set to non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Mask>: Specified mask
route-filter: Non-masked bits not zero for <Address> masklen <Masklen>	At masklen, 1 is set to non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Masklen>: Specified mask length
route-filter: not IPv6 prefix	Addresses other than an IPv6 prefix are specified. Specify IPv6 prefix.
route-filter: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
route-filter: route-filter name "<Name>" longer than 15 characters	The specified ID exceeds 15 characters. Specify ID by 15 or less characters.
	<Name>: specified ID
route-filter: route-filter sequence out of order	The specified order of a sequence number is incorrect. Specify a in ascending sequence.
route-filter: Set-attribute not found at <Value>	The specified ID number is not defined. Specify a defined ID number
	<Value>: Specified ID number
route-filter: syntax error	Syntax error

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

routerid: address invalid for routerid	The router ID is illegal. Specify a value other than 0.0.0.0/8, 127.0.0.0/8, and 240.0.0.0/24.
routerid: error resolving '<Host Name>': Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host Name>: Specified host name
routerid: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
routerid: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
routerid: routerid specified twice	routerid: routerid specified twice
routerid: syntax error	Syntax error
static: address should not be::	Default address is specified in the address. Specify addresses other than the local host address.
static: address should not be v4-compat	The extended community is duplicated for definition. Do not duplicate the extended community for definition.
static: address should not be v4-mapped	An IPv4-compatible address is specified in an address. Specify addresses other than the IPv4-compatible address.
static: destination <IPv6 Prefix> and gateway <Address> must belong to the same address family	The address is defined in gateway address other than IPv6 prefix. Specify IPv6 prefix.
	<IPv6 Prefix>: Specified destination address <Address>: Specified gateway address
static: duplicate gateway in list at <Address>	In the static definition, a gateway address is duplicated. Specify a unique gateway address.
	<Address>: Specified gateway address
static: duplicate preference <Value> static route to <Address>	Preference value static route is duplicated in a destination. Use a unique static route.
	<Value>: specified preference value <Address>: Specified static route address
static: error resolving '<Host Name>': Unknown host	The specified host name cannot be found. Specify the defined host name.
	<Host Name>: Specified host name
static: gateway not a host address on an attached network: <Address>	Specified gateway is not the address of the host on the connected network. Specify a gateway address on the specified interface address.
	<Address>: Specified gateway address
static: gateway <IPv6 Prefix> is not global/ site-local/linklocal IPv6 address	Specified gateway address is invalid. Specify global/site-local/ linklocal address.
	<IPv6 Prefix>ÅFSpecified gateway address
static: Interface not found at '<Interface Name>'	The specified interface name cannot be found. Specify the defined interface name.
	<Interface Name>: specified interface name
static: Interface not found at <Address>	Interface of specified interface address is not found. Use a defined interface address.
	<Address>: Specified interface address
static: invalid inet mask bits value at <Masklen> not in range 0 to {32|128}	In the masklen specification, the mask length is invalid. Specify a value within the range of 0 to 32/128.
	<Masklen>: Specified mask length
static: Invalid interface name '<Interface Name>'	The multi-home interface is specified. Do not specify multi-home interface.
	<Interface Name>: specified interface name

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

static: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
static: invalid pollcount value at xxx not in range 1 to 10	Polling count is out of valid range. Specify value within the range of 1 to 10.
	<Value>: Specified polling count
static: invalid pollinterval value at <Value> not in range 5 to 180	Polling timer value is out of valid range. Specify value within the range of 5 to 180.
	<Value>: Specified polling timer value
static: Invalid pollinterval	Polling timer value is invalid. Specify value in the multiples of 5.
static: invalid preference value at <Value> not in range 2 to 255.	Preference value is invalid. Specify a value within the range of 2 to 255.
	<Value>: Specified preference value.
static: invalid vpn number value at <Value> not in range 1 to <Max_Value>	VPN number is out of valid range. Specify value within the range of 1 to <Max_Value>.
	<Value>: Specified VPN number <Max_Value>Maximum VPN number
static: IPv6 prefix cannot be linklocal in configuration	The link local address is specified in the network address. Do not use the link local address.
static: IPv6 prefix cannot be multicast in configuration	The multicast address is specified in the network address. Do not use the multicast address.
static: IPv6 static interface statement should be used for non- broadcast I/F	The broadcast interface is specified in the specified interface in the static definition. To specify the interface, specify the point-to-point interface.
static: linklocal address should be followed by %(IPv6 interface name)	An interface name is not specified in the specified link local address. Specify an interface name with the percent (%) interposed when specifying a link local address.
static: mask not contiguous	Bit 1 of the specified mask does not continue. Use a mask where bit 1 continues.
static: multipath option not valid for vpn route	The multipath option has been defined relative to the VPN route. Do not define the multipath option relative to the VPN route.
static: Non-masked bits not zero for <Address> mask <Mask>	In the mask specification, 1 is set to the non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Mask>: Specified mask
Static: Non-masked bits not zero for <Address> masklen <Masklen>	In the masklen specification, 1 is set to the non-masked bit of the specified address. Set non-masked bit 0.
	<Address>: Specified address <Masklen>: Specified mask length
static: not IPv6 prefix	Addresses other than an IPv6 prefix are specified. Specify IPv6 prefix.
static: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
static: poll option not valid for vpn remote-gateway	Polling option is defines in a VPN remote route. Do not define a polling option in a VPN remote route.
static: remote-gateway <IPv6 Prefix> is not global/site-local IPv6 address	Addresses other than a global address or site local address are specified. Specify the global address or site local address for remote-gateway. <IPv6 Prefix>: Specified local address
static: syntax error	Syntax error
The total number of {targets|IPv6 static gateways} (<Value>) is more than the maximum permitted (256)	Total number of specified targets is more than maximum acceptable value. Specify a number up to 256.
	<Value>: Total number of specified targets

Downloaded from www.Manualslib.com manuals search engine

Table 5-5 Routing Protocol Error Messages (continued)

vpnmap: address invalid for routerid	Router ID is invalid. Specify other than 0.0.0.0/8, 127.0.0.0/8, 240.0.0.0/24.
vpnmap: duplicate extended community.	Extended community is duplicated. Specify a unique extended community.
vpnmap: duplicate vpn at <Value>	Vpn number is duplicated. Specify a unique vpn number.
	<Value>: Specified vpn number
vpnmap: error resolving '<Host Name>': Unknown host	Specified host name is not founded. Specify a defined host name
	<Host Name>: Specified host name
vpnmap: invalid autonomous system number value at <Value> not in range 1 to 65534	Specified range of AS number in RD or the extended community is invalid. Specify in the range of 1 to 65534.
	<Value>: Specified AS number
vpnmap: invalid index number in extended community number value at <Value> not in range 0 to 65535 / 4294967295	Specified range of ID number in extended community is invalid. Specify in the range of 0 to 65535, or 0 to 4294967295.
	<Value>: Specified ID number
vpnmap: invalid index number in rd value at <Value> not in range 0 to 65535 / 4294967295	Specified range of ID number in RD is invalid. Specify in the range of 0 to 65535, or 0 to 4294967295.
	<Value>: Specified ID number
vpnmap: invalid max_local_routes number value at <Value> not in range 1 to 65535	Specified range of max routes number is invalid. Specify in the range of 1 to 65535.
	<Value>: Specified max routes number
vpnmap: invalid max_routes number value at <Value> not in range 1 to 65535	Specified range of max routes number is invalid. Specify in the range of 1 to 65535.
	<Value>: Specified max routes number
vpnmap: invalid number of extended communities value at <Value> not in range 1 to 25	The defined number of extended community exceeds defined max number. Specify number by 25 or less characters.
	<Value>: defined number of extended community
vpnmap: invalid octet value at <Value> not in range 0 to 255	More than 255 values are defined in dot notation. Specify value within the range of 0 to 255.
	<Value>: Specified value
vpnmap: invalid vpn number value at <Value> not in range 1 to <Max_Value>	Specified range of VPN number is invalid. Specify in the range of 1to <Max_Value>
	<Value>: Specified vpn number <Max_Value>Maximum VPN number
vpnmap: invalid warning_local_routes number value at <Value> not in range 1 to 65535	Specified range of warning local routes number is invalid. Specify in the range of 1 to 65535.
	<Value>: Specified warning local routes number
vpnmap: invalid warning_routes number value at <Value> not in range 1 to 65535	Specified range of warning local routes number is invalid. Specify in the range of 1 to 65535.
	<Value>: Specified warning local routes number
vpnmap: out of range	The parameter-specified range is exceeded in the input command syntax. Numeric values of more than 4294967296 are contained. Reconfirm a parameter.
vpnmap: Relations between local address and destination ip address in ip configuration are inconsistent	The relation between the local address, and the IP address and destination IP address of IP is inconsistent. Set a local address that differs from the IP address and destination IP address of IP (in case of VPN-undefined IP).
vpnmap: syntax error	Syntax error

Downloaded from www.Manualslib.com manuals search engine

5.6 Multicast Routing Protocol

Table 5-6 Multicast Router Control Information Error Messages

Message	Contents
configuration check error	Configuration definition check has failed.
dvmrp: can not locate tunnel on interface	The interface defined by the DVMRP tunnel cannot be defined. Specify the interface address other than the DVMRP tunnel.
dvmrp: can not set interface address at <Address>	The interface addresses specified in the dvmrp definition cannot be set. Do not specify the following interfaces because they are not supported in the multicast. (1) Interface of RM Ethernet (2) Interface of AUX(RS232C) (3) Interface in which the IP interface type is broadcast type in other than LAN/WAN (PPP). (4) Shared address interface. (5) Local loop-back interface (6) Null interface. (7) Router device address (device address set by using the config router command). (8) Tunnel interface.
	<Address>: Specified interface address.
dvmrp: duplicate dvmrp clause	dvmrp definition is duplicated. Delete one definition.
dvmrp: duplicate interface address in list at <Address>	Interface address is duplicated in dvmrp definition. Specify not to duplicate interface address.
	<Address>: Specified interface address
dvmrp: Interface not found at <Address>	Interface of specified interface address is not found. Use a defined interface address.
	<Address>: Specified interface address
dvmrp: invalid DVMRP metric value at <Metric> not in range 1 to 32	The specified DVMRP metric value in dvmrp definition is invalid. Specify within the range of 1 to 32.
	<Metric>: Specified metric value
dvmrp: invalid inet mask length for interface <address> not in range 8 to 32	The mask length of the interface defined for DVMRP exceeds the permissible range. Set the mask length of the interface to 8 through 32.
	<Address>: Specified interface address
dvmrp: octet or hex string too long to be an IP address	The specified IP address format is invalid. Specify in correct dot format.
dvmrp: the total number of enable interfaces is more than the maximum permitted (32)	The total number of defined and enabled interfaces exceeds the permissible maximum number. Set to 32 or less the number DVMRP tunnel definitions in dvmrptunnel plus the number of the addresses of interfaces set to “enable” in dvmrp definitions.
dvmrp: the total number of enable virtual interface is more than the maximum permitted (32)	The total number of virtual interfaces exceeds the maximum permissible number. Set to 32 or less the number DVMRP tunnel definitions in dvmrptunnel plus the number of the addresses of interfaces set to “enable” in igmp or dvmrp definitions.
dvmrp: the total number of interfaces is more than the maximum permitted (32)	The total number of the DVMRP tunnels specified in the dvmrptunnel definition has exceeded the maximum allowance. Specify the tunnels so that the number of definition for the DVMRP tunnels in the dvmrptunnel definition is 32 or less.
dvmrptunnel: duplicate dvmrptunnel clause	In the dvmrptunnel definition is duplicated. Delete one definition.
dvmrptunnel: duplicate remote address: <Remote address> PointToPoint	The remote address specified in dvmrptunnel definition is duplicated. Specify not to duplicate remote address.
	<Remote address>: Specified remote address

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

dvmrptunnel: error resolving <Address>: Unknown host	The interface address specified in dvmrptunnel definition is invalid. Specify the correct interface address.
	<Address>: specified interface address
dvmrptunnel: octet or hex string too long to be an IP address	The specified IP address format is invalid. Specify in correct dot format.
dvmrptunnel: specified remote address <Address> belongs to the local network of this router	The specified remote address is the local network of this device. Use network address other than local address of this device for remote address.
	<Address>: Specified remote address
dvmrptunnel: the total number of enable interfaces is more than the maximum permitted (32)	The total number of the DVMRP tunnels specified in the dvmrptunnel definition has exceeded the maximum allowance. Specify the tunnels so that the number of definition for the DVMRP tunnels in the dvmrptunnel definition is 32 or less.
dvmrptunnel: the total number of enable virtual interface is more than the maximum permitted (32)	The total of specified multicast tunnel in dvmrptunnel definition exceeds the maximum permitted. Specify multicast tunnel definition count in dvmrptunnel definition to 32 or less.
dvmrptunnel: tunnel <Remote address> has bad local address <Local address>	In the dvmrptunnel definitions, there is no local address for the specified remote address or local addresses are not supported. For the local address, specify the defined interface address. Do not specify the following interfaces because they are not supported in the multicast. (1) Interface of RM Ethernet (2) Interface of AUX(RS232C) (3) Shared address interface. (4) Local loop-back interface (5) Null interface. (6) Router device address (device address set by using the config router command). (7) Tunnel interface.
	<Remote address>: Specified remote address. <Local address>: Specified local address.
dvmrptunnel: tunnel has bad remote address <Address>	The specified remote address is invalid. Specify the correct remote address.
	<Address>: Specified remote address.
igmp: can not locate tunnel on interface	The interface defined by the DVMRP tunnel cannot be defined. Specify the interface address other than the DVMRP tunnel.
igmp: can not set interface address at <Address>	The interface addresses specified in the igmp definition cannot be set. Do not specify the following interfaces because they are not supported in the multicast. (1) Interface of RM Ethernet (2) Interface of AUX(RS232C) (3) Interface in which the IP interface type is broadcast type in other than LAN/WAN (PPP). (4) Shared address interface. (5) Local loop-back interface (6) Null interface. (7) Router device address (device address set by using the config router command). (8) Tunnel interface.
	<Address>: Specified interface address.
igmp: duplicate igmp clause	The igmp definition is duplicated. Delete one definition.
igmp: duplicate interface address in list at <Address>	The interface address in igmp is duplicated. Specify not to duplicate interface address.
	<Address>: Specified interface address

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

igmp: Interface not found at <Address>	The interface of interface address specified in igpm definition cannot be found. Specify the defined interface address.
	<Address>: Specified interface address
igmp: invalid max-response-time value at <Value1> not in range 1 to <Value2>	The specified Query message response waiting time in igmp definition is invalid. Specify within the range of 1 to (Query message transmission interval - 1). The maximum Query message response waiting time is 25.
	<Value1>: Specified Query message response waiting time <Value2>: Query message transmission interval-1(it shows 25 when query message transmission interval-1is more than 25).
igmp: invalid inet mask length for interface <address> not in range 8 to 32	The mask length of the interface defined for IGMP exceeds the permissible range. Set the mask length of the interface to 8 through 32.
	<Address>: Specified interface address
igmp: invalid query-interval value at <Value1> not in range <Value2> to 65535	The specified Query message transmission interval in igmp definition is invalid. Specify within the range of (Query message response waiting time + 1) to 65535.
	<Value>: Specified Query message transmission interval <Value2>: Query message response waiting time + 1
igmp: invalid seconds value at <Value> not in range 0 to 65535	The specified timer value in igmp definition is invalid. Specify within the range of 0 to 65535.
	<Value>: Specified timer value
igmp: octet or hex string too long to be an IP address	The format of specified IP address is invalid. Specify in the correct dot format.
igmp: the total number of enable virtual interface is more than the maximum permitted (32)	The total number of interface addresses specified in the igmp definition has exceeded the maximum allowance. Set to 32 or less the number of DVMRP tunnel definitions in dvmrptunnel plus the number of the addresses of interfaces set to “enable” in the igmp or dvmrp definition.
igmp: the total number of interfaces is more than the maximum permitted (32)	The total number of interface addresses specified in the igmp definition has exceeded the maximum allowance. Specify the addresses so that the number of interface addresses specified in the igmp definition is 32 or less.
Multicast and MPLS can not be set up simultaneously.	Multcast and MPLS can not be set up simultaneously
multicast:<address> is not in agreement with the group address set up by ssm	The range of the group address set by the "ssm-join" command does not coincide with the range of the group address set by the "ssm " command.
	<address>: local address set by the "ssm-join" command
multicast:address of group definition is not omissible	No group address is specified on the "smm-join" command definition.
multicast:address of source definition is not omissible	No local address is specified in the "ssm-join" command.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

multicast: can not set interface address at <Address>	The interface addresses specified in the multicast definition cannot be set. Do not specify the following interfaces because they are not supported in the multicast. (1) Interface of RM Ethernet (2) Interface of AUX(RS232C) (3) Interface in which the IP interface type is broadcast type in other than LAN/WAN (PPP). (4) Shared address interface. (5) Local loop-back interface (6) Null interface. (7) Router device address (device address set by using the config router command). (8) Tunnel interface.
	<Address>: Specified interface address.
multicast: duplicate group address with the same mask at <Group address>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Perform specification by using any one of the following forms so that the combination of the multicast group address and mask will not be duplicated. (1)<Group address> (2)<Group address>/<Masklen> (<Masklen>: Mask length) (3)<Group address> masklen <Masklen> (<Masklen>: Mask length) (4) <group address> mask <Mask> (<Mask>: Mask) Perform specification so that the definition will not be duplicated also in the group addresses specified in the join and the staticjoin.
	<Group address>: Specified multicast group address.
multicast: duplicate group address with the same mask at <Group address> / <Masklen>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Perform specification by using any one of the following forms so that the combination of the multicast group address and mask will not be duplicated. (1) <Group address> (2) <Group address>/<Masklen>(<Masklen>: Mask length) (3) <Group address> masklen <Masklen>(<Masklen>: Mask length) (4) <group address> mask <Mask>(<Mask>: Mask) Perform specification so that the definition will not be duplicated also in the group addresses specified in the join and the staticjoin.
	<Group address>: Specified multicast group address. <Masklen>: Specified mask length.
multicast: duplicate group address with the same mask at <Group address> masklen <Masklen>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Perform specification by using any one of the following forms so that the combination of the multicast group address and mask will not be duplicated. (1) <Group address> (2) <Group address>/<Masklen>(<Masklen>: Mask length) (3) <Group address> masklen <Masklen>(<Masklen>: Mask length) (4) <group address> mask <Mask>(<Mask>: Mask) Perform specification so that the definition will not be duplicated also in the group addresses specified in the join and the staticjoin.
	<Group address>: Specified multicast group address. <Masklen>: Specified mask length.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

multicast: duplicate group address with the same mask at <Group address> mask <Mask>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Perform specification by using any one of the following forms so that the combination of the multicast group address and mask will not be duplicated. (1) <Group address> (2) <Group address>/<Masklen>(<Masklen>: Mask length) (3) <Group address> masklen <Masklen>(<Masklen>: Mask length) (4) <group address> mask <Mask>(<Mask>: Mask) Perform specification so that the definition will not be duplicated also in the group addresses specified in the join and the staticjoin.
	<Group address>: Specified multicast group address. <Mask>: Specified mask.
multicast:duplicate group <address> clause	Duplicate group addresses are specified by the "ssm-join" command.
	<address>: group address specified by the "ssm-join" command
multicast:duplicate source <address> clause	Duplicate local addresses are specified within the same "ssm-join" command
	<address>: local address specified by the "ssm-join" command
multicast: duplicate interface address at <Address> for <Group address>	interface addresses are defined in duplication in the same multicast group address in the multicast definition. Specify the address so that the interfaces defined in the multicast group address are not duplicated.
	<Address>: Specified interface address. <Group address>: Specified multicast group address.
multicast: duplicate interface address at <Address> for <Group address> / <Masklen>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Specify the address so that the interfaces defined in the multicast group address are not duplicated.
	<Address>: Specified interface address. <Group address>: Specified multicast group address. <Masklen>: Specified mask length.
multicast: duplicate interface address at <Address> for <Group address> masklen <Masklen>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Specify the address so that the interfaces defined in the multicast group address are not duplicated.
	<Address>; Specified interface address. <Group address>: Specified multicast group address. <Masklen>: Specified mask length.
multicast: duplicate interface address at <Address> for <Group address> mask <Mask>	Interface addresses are defined in duplication in the same multicast group address in the multicast definition. Specify the address so that the interfaces defined in the multicast group address are not duplicated.
	<Address>: Specified interface address. <Group address>: Specified multicast group address. <Mask>: Specified mask.
multicast: duplicate multicast clause	multicast definition is duplicated. Delete one definition.
multicast:duplicate ssm-join clause	Multiple "ssm-join" commands have been defined. The maximum number is 1.
multicast: error resolving <Group address> : network unknown	The group address specified in multicast definition is invalid. Specify the correct group address.
	<Group address>: Specified group address.
multicast: Interface not found at <Address>	The interface name specified in multicast definition cannot be found. Specify the defined interface address.
	<Address>: Specified interface address.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

multicast: invalid inet mask bits value at <Masklen> not in range 4 to 32	The specified mask length in multicast definition is invalid. Specify within the range of 4 to 32.
	<Masklen>: Specified mask length.
multicast: mask length out of range from 4 to 32	The specified mask pattern in multicast definition is invalid. Specify mask pattern with length of 4 to 32.
multicast: mask not contiguous	The specified mask in multicast definition is not contiguous with bit 1. Specify the mask that bit 1 is contiguous.
multicast: Non-masked bits not zero for <Group address> / <Masklen>	1 is set to non-masked bits of address for masklen specification in multicast definition. Specify 0 to non-masked bits.
	<Group address>: Specified multicast group address. <Masklen>: Specified mask length.
multicast: Non-masked bits not zero for <Group address> mask <Mask>	1 is set to non-masked bits of address for mask specification in multicast definition. Specify 0 to non-masked bits.
	<Group address>: Specified multicast group address. <Mask>: Specified mask.
multicast: Non-masked bits not zero for <Group address> masklen <Masklen>	1 is set to non-masked bits of address for masklen specification in multicast definition. Specify 0 to non-masked bits.
	<Group address>: Specified multicast group address. <Masklen>: Specified mask length.
multicast: octet or hex string too long to be an IP address	The specified IP address format is invalid. Specify in the correct dot format.
multicast:ssm-join is not supported in DVMRP, IGMP, DVMRPTUNEL.	The "ssm-join" command is defined when using DVMRP, IGMP and DVMRPTUNEL.
multicast:The combination total of GROUP and SOURCE exceeded the maximum permitted	The sum total of groups and sources defined by "ssm-join" exceeds the allowable limit. Set the sum total of groups and sources to a maximum of 256.
multicast:join and staticjoin are not supported in PIN-SM	"join" and "staticjoin" are not supported with PIM-SM.
multicast: the parameter must be a group address (class D)	The group address specified in multicast definition is invalid. Specify the group address by IP address of class D.
multicast: this address is not supported <Group address>	The specified group address in multicast definition is not supported. Specify the group address by IP address of class D.
	<Group address>: Specified multicast group address.
multicast:this source address is not supported <Source address>	The range for specifying local addresses specified by "ssm-join" is invalid. Specify IP addresses of classes A - C.
	<Source address>: local address specified by the "ssm-join" command
PIM and DVMRP can not be set up simultaneously.	The PIM and the DVMRP cannot be set simultaneously. Define only either one of the PIM information (pim) or the DVMRP information (igmp, dvmrp, dvmrptunnel).
PIM-SM and multicast can not be set up simultaneously.	PIM-SM does not support multicast settings.
pim: can not check configuration, please try again	The configuration definition cannot be checked because actuation of the multicast routing program has not been completed. Try it again after some time.
pim: can not set candidate-bsr on this router which is not configured to router local_address	Unless the device address is defined, there is no setting BSR candidates. First set the device address.
pim: can not set candidate-rp on this router which is not configured to router local_address	Unless the device address is defined, there is no setting rendezvous point candidates. First set the device address.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

pim: can not set interface address at <Address>	The interface addresses specified in the pim definition cannot be set. Do not specify the following interfaces because they are not supported in the multicast. (1) Interface of RM Ethernet (2) Interface of AUX(RS232C) (3) Interface in which the IP interface type is broadcast type in other than LAN/WAN (PPP). (4) Shared address interface. (5) Local loop-back interface (6) Null interface. (7) Router device address (device address set by using the config router command). (8) Point-point type interface in which the destination IP address is not specified. (9) Tunnel interface.
	<Address>: Specified interface address.
pim: dense and sparse can not be set up simultaneously	Simultaneous settings of PIM-DM and PIM-SM are not permitted.
pim: duplicate group address and mask <Group address> / <Masklen>	The group address and the mask length of specified rendezvous point candidates have already been defined.
	<Group address>: Specified multicast group address <Masklen>: Specified mask length
pim: duplicate interface address in list at <Address>	Interface address is duplicated in pim definition. Specify not to duplicate interface address.
	<Address>: Specified interface address.
pim: duplicate pim clause	pim definition is duplicated. Delete one definition.
pim: duplicate sparse parameter	sparse definition is duplicated. Delete one definition.
pim:duplicate ssm clause	Multiple PIM-SSM "ssm" commands are defined. The maximum number is 1.
pim: Interface not found at <Address>	The interface of interface address specified in pim definition cannot be found. Specify the defined interface address.
	<Address>: Specified interface address.
pim: invalid candidate-bsr priority value at '<Num>' not in range 0 to 255	The priority of BSR candidates exceeds the permissible range. Specify a value from 0 through 255.
	<Num>: Specified priority
pim: invalid candidate-rp priority value at '<Num>' not in range 0 to 255	The priority of rendezvous point candidates exceeds the permissible range. Specify a value from 0 through 255.
pim: invalid dense name	specified in pim definition is invalid. Enter dense name with 1 to 14 characters.
pim: invalid inet mask bits value at <Masklen> not in range 4 to 32	The specified range of the mask length set for rendezvous point candidates for PIM-SM is illegal. Specify a value from 4 through 32.
	<Masklen>: Specified mask length
pim: invalid interface address at <Address>	The interface address value specified in pim definition is invalid. Enter the correct interface address.
	<Address>: Specified interface address.
pim: local address and remote address belong to different subnets on PointToPoint interface <Address>	In the point-to-point interface, different subnets are set for the local address and the remote address. To operate PIM with the point-to-point interface, use the same subnet.
	<Address>: Specified interface address
pim: mask length out of range from 4 to 32	The mask pattern specified for rendezvous point candidates of PIM-SM exceeds the permissible range. Specify a mask pattern with a mask length of 4 through 32.
pim: invalid inet mask length for interface <address> not in range 8 to 30	The mask length of the interface defined for PIM exceeds the permissible range. Set the interface mask length to 8 through 30.
	<Address>: Specified interface address

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

pim: invalid max-interfaces value at '<Num>'	PIM-SM does not support max-interfaces values.
	<Num>: The maximum number of specified interfaces
pim: mask not contiguous	The specified mask for rendezvous point candidates of PIM-SM is not continuous at bit 1. Specify a mask that is continuous at bit 1.
pim: Non-masked bits not zero for <Group address> / <Masklen>	In the group of rendezvous point candidates of PIM-SM, the non-mask bit of the specified masklen address is set to "1." Set the non-mask bit to "0."
	<Group address>: specified multicast group address <Masklen>: Specified mask length
pim: Non-masked bits not zero for <Group address> mask <Mask>	In specifying a mask for the group of rendezvous point candidates of PIM-SM, the non-mask bit of the specified address is set to "1." Set the non-mask bit to "0."
	<Group address>: specified multicast group address <Mask>: Specified mask
pim: Non-masked bits not zero for <Group address> masklen <Masklen>	In specifying masklen for the group of rendezvous point candidates of PIM-SM, the non-mask bit of the specified address is set to "1." Set the non-mask bit to "0."
	<Group address>: specified multicast group address <Masklen>: Specified mask length
pim: octet or hex string too long to be an IP address	The specified IP address format is abnormal. Specify the correct dot format.
pim:ssm is not defined	Though the "ssm-join" command has been defined, the "ssm" command has not been defined.
pim: the parameter must be a group address (class D)	The group address specified for rendezvous point candidates of PIM-SM is illegal. For the group address, specify a Class-D IP address.
pim: the total number of enable interfaces is more than the max-interfaces value (<Num>)	The total number of interface addresses specified to be enable in the pim definition has exceeded the value specified by max-interfaces (<Num>). Specify the addresses so that the number of interface addresses specified to be enable is less than the value specified by max-interfaces (<Num>). The maximum value for the max-interfaces is 256. If addition of the interface definition for PIM is wanted, add the definition after having increased the value of the max-interfaces. If deletion the interface definition of PIM is wanted, delete the interface definition so that the number of interface addresses specified to be enable is less than the value of the max-interfaces (<Num>).
	<Num>: Specified number of the maximum interfaces.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

pim: the total number of enable interfaces is more than the max-interfaces value (<Num1>) though it is less than the maximum number of interfaces that this router runs (<Num2>)	The total number of interface addresses specified to be enable in the pim definition is less than the maximum number of the interfaces in which this device is operating (<Num2>), but the value specified by the max-interfaces (<Num1>) has been exceeded. Specify the addresses so that the number of interface addresses specified to be enable is less than the number (<Num1>). If addition of the interface definition is wanted, add it using the following procedure: (1) Increase the value of the max-interface. However, the maximum value for the max-interface is 256. (2) Execute the config apply command. (3) Execute the Operations Guide -New Syntax Operation Command, Vol. 1- restart ipv4-multicast command. (4) Add the interface address of PIM. If deletion of the interface definition is wanted, add it using the following procedure: (1) Delete the interface definition so that the number of interface addresses specified to be enable is less than the value of the max interfaces (<Num1>). (2) Decrease the value for the max-interfaces. However, the minimum value for the max-interfaces is 32. (3) Execute the config apply command. (4) Execute the restart ipv4-multicast command.
	<Num1>: Maximum number of interfaces in which this device is operating. <Num2>: Maximum specified number of interfaces
pim: the total number of enable interfaces is more than the max-interfaces value at the config apply command execution (<Num>)	The total number of interface addresses specified to be enable in the pim definition has exceeded the value of the max-interfaces when the config apply command has been executed in the previous run (<Num>). If change in the value of the max-interfaces is wanted execute the config apply command and the restart ipv4-multicast command in that order. (1) Execute the config apply command. (2) Execute the restart ipv4-multicast command. (3) Add the interface address.
	<Num>: The maximum number of specified interface at executing config apply command last time.
pim: the total number of enable interfaces is more than the maximum permitted (32)	The total number of interface addresses specified in the pim definition has exceeded the maximum allowance. Specify the addresses so that the number of enable interface addresses of PIM is 32 or less.
pim: the total number of enable interfaces is more than the maximum number of interfaces that this router runs (<Num>)	In PIM definitions, the total number of interface addresses set to “enable” exceeds the maximum number of interfaces run on the system (<Num>). Set the number of enable-specified interface addresses to <Num> or less. To add an interface definition, take the following steps: (1) Increase the value of max-interfaces. The value can be increased up to 256. (2) Execute the config apply command. (3) Execute the restart ipv4-multicast command. (4) Add interface addresses for PIM.
	<Num>: The maximum number of interfaces run on the system.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Multicast Router Control Information Error Messages (continued)

pim: the total number of enable interfaces is more than the maximum number of interfaces that this router runs (<Num1>) though it is less than the max-interfaces value (<Num2>)	The total number of interface addresses set to “enable” in the PIM definition does not exceed the value (<Num2>) specified for max-interfaces. But the number exceeds the maximum number of interfaces running on the system (<Num1>). Set the number of enable-specified interface addresses to <Num1> or less. To add an interface definition, take the following steps: (1) Execute the config apply command. (2) Execute the restart ipv4-multicast command. (3) Add an interface address of PIM.
	<Num1>: The maximum number of interfaces running on the system. <Num2>: The number of specified interfaces.
pim: the total number of groups on candidate-rp is more than the maximum permitted (128)	The total number of group addresses of rendezvous point candidates exceeds the maximum capacity. Specify 128 addresses or less.
pim: the total number of interfaces is more than the maximum permitted (<Num>)	The total number of interface addresses specified in the PIM definition exceeds the maximum capacity. Set the number of PIM addresses to <Num> or less.
	<Num>: The maximum number of specified interfaces
pim:the number of PIM-SSM groups is set up exceeding the maximum	The number of PIM-SSM group addresses that have been set exceeds the maximum limit. The maximum number is 1.
pim: this address is not supported <Group address>	The group address specified for PIM-SAM rendezvous point candidates is not supported. For the group address, specify a Class-D IP address.
	<Group address>: Specified multicast group address
<Command>: syntax error	Syntax error
	<Command>: Command name

Downloaded from www.Manualslib.com manuals search engine

5.7 IPv6 Multicast Routing Protocol

Table 5-7 IPv6 Multicast Router Control Information Error Messages

Message	Contents
configuration check error	Configuration definition check has failed.
mld:address of group definition is not omissible	No group address is specified on the "smm-join" command definition.
mld:address of source definition is not omissible	No local address is specified in the "ssm-join" command.
mld:<address> is not in agreement with the group address set up by ssm	The range of the group address set by the "ssm-join" command does not coincide with the range of the group address set by the "ssm " command.
	<address>: local address set by the "ssm-join" command
mld:duplicate group <address> clause	Duplicate group addresses are specified by the "ssm-join" command.
	<address>: local address set by the "ssm-join" command
mld:duplicate source <address> clause	Duplicate local addresses are specified within the same "ssm-join" command
	<address>: local address set by the "ssm-join" command
mld:duplicate ssm-join clause	Multiple "ssm-join" commands have been set. The maximum number is 1.
mld:Source prefix(<IPv6 Source address>) has a narrow scope	The range for specifying local addresses specified by the "ssm-join" command is invalid. Specify IPv6 addresses other than local addresses.
	<IPv6 source address>: local address specified by the "ssm-join" command
mld:The combination total of GROUP and SOURCE exceeded the maximum permitted.	The sum total of groups and sources defined by "ssm-join" exceeds the allowable limit. Set the sum total of groups and sources to a maximum of 256.
pim:<IPv6 Group Prefix> is not an IPv6 multicast address	Group addresses specified by IPv6 PIM-SM rendezvous point candidates must be multicast addresses. Or the group address specified by the "ssm-join" command of PIM-SSM is not an IPv6 multicast address.
	<IPv6 group prefix>: Specified IPv6 multicast group address
pim:prefix length <Prefixlen> should be ranged between 8 and 128	The range for specifying prefix length specified by IPv6 PIM-SM rendezvous point candidates is invalid. Or the range for specifying prefix length specified by PIM-SMM group address is invalid. Set within the range of 8 - 128.
	<Prefixlen>: Specified prefix length
pim6: already defined enable or disable for <Interface Name>	In pim6 definition, enable or disable is specified for the same interface two times or more. Specify enable or disable only once.
pim6: candidate-bsr is already defined	candidate-bsr of pim6 is duplicate-defined. Delete one of the definitions.
pim6: candidate-bsr priority is already defined	candidate-bsr priority of pim6 is duplicate-defined. Delete one of the definitions.
pim6: candidate-bsr priority value '<Num>' should be ranged between 0 and 255	The priority level of a BSR candidate is out of the range. Set a value of 0 to 255.
	<Num>: Set priority level
pim6: candidate-rp is already defined	candidate-rp of pim6 is duplicate-defined. Delete one of the definitions.
pim6: candidate-rp priority is already defined	candidate-rp priority of pim6 is duplicate-defined. Delete one of the definitions.
pim6: candidate-rp priority value '<Num>' should be ranged between 0 and 255	The priority of rendezvous point candidates exceeds the permissible range. Specify a value from 0 through 255.

Downloaded from www.Manualslib.com manuals search engine

Table 5-7 IPv6 Multicast Router Control Information Error Messages (continued)

pim6: duplicate group prefix <IPv6 Group Prefix> / <Prefixlen>	The prefix of the specified rendezvous point candidate has already been defined.
	<IPv6 Group Prefix>: Specified IPv6 multicast group address <Prefixlen>: Specified prefix length
pim6: duplicate pim6 clause	pim6 definition is duplicated. Delete one definition.
pim6: duplicate sparse parameter	sparse definition is duplicated. Delete one definition.
pim6: global or site local address not assigned on router local address	Unless the device address is defined, there is no setting pim6. First set the device address.
pim6: group prefix(<IPv6 Group Prefix>) has a narrow scope	The group address specified by the rendezvous point candidate of IPv6 PIM-SM must have a wider scope than the link local address. Set the scope of the group address to 3 or more.
	<IPv6 Group Prefix>: Specified IPv6 multicast group address
pim6: interface <Interface Name> is already defined	The interface address is duplicate-defined in pim6 definition. Specify it so that the interface address is not duplicated.
	<Interface Name>: Specified interface name
pim6: interface <Interface Name> not found	The interface of the interface name specified in pim6 definition cannot be found Specify the interface by the defined interface name.
	<Interface Name>: Specified interface name
pim6: invalid IPv6 address: <IPv6 Address>	The format of the specified IPv6 address is invalid. Specify the address in a proper format.
	<Prefixlen>: Specified address
pim6: the number of active pim6 interfaces (<Num>) should be less than 32	The total number of enable-specified interface addresses in pim6 definition exceeds the maximum allowable number of addresses. Specify so that the number of enable-specified interface addresses is less than 32.
	<Num>: Number of enable-defined interfaces in pim6 configuration definition
pim6:ssm is not defined	Though the "ssm-join" command has been defined, the "ssm" command has not been defined.
pim6:the number of PIM-SSM groups is set up exceeding the maximum	The number of group addresses of IPv6 PIM-SSM exceeds the allowable limit. The maximum number is 1.
pim6: the total number of group prefix should not be greater than 128	The total number of IPv6 group addresses in a rendezvous point candidate exceeds the maximum number of addresses. Set so that the total number of group addresses is within 128.
pim6: unsupported interface <Interface Name> specified	The interface specified in pim6 definition cannot be set. Do not specify the interfaces below because they are not supported in an IPv6 multicast. 1. Interface in which IPv6 address cannot be defined 2. Tunnel interface
	<Interface Name>: Specified interface name
<Command>: syntax error	Syntax error
	<Command>: Command name\

Downloaded from www.Manualslib.com manuals search engine

5.8 Flow Information Error Messages

Table 5-8 Flow Information Error Messages

Message	Contents
Can not change cops_range.	The list number cannot be changed because it has already been used in a COPS function. Define cops no or delete the COPS configuration definition. [Ver.06-03]
Can not delete all action because premium is defined.	The action cannot be deleted totally because the important packet flow detecting conditions (premium) have been defined. Input all the detecting conditions again to nullify the Action.
Can not delete flow list because COPS used.	The list number cannot be changed because it has already been used in a COPS function. Define cops no or delete the COPS configuration definition. [Ver.06-03]
Can not delete flow qos, flow filter because COPS used.	The list number cannot be changed because it has already been used in a COPS function. Define cops no or delete the COPS configuration definition. [Ver.06-03]
Can not delete IP configuration referred by flow filter configuration.	The following factors are conceivable. 1).The specified interface cannot be deleted because the interface name specified in the flow filer has already been set. To delete the specified interface, it is necessary to delete the interface name specified in the flow filter. 2).The designated interface cannot be deleted because an interface name that has set the data from a policy server using the COPS function has been set. To delete the designated interface, delete the designated interface's data set from the policy server.
Can not delete IP configuration referred by flow qos configuration.	The following factors are conceivable. 1).The specified interface cannot be deleted because the interface name specified in the flow filer has already been set. To delete the specified interface, it is necessary to delete the interface name specified in the flow filter. 2).The designated interface cannot be deleted because an interface name that has set the data from a policy server using the COPS function has been set. To delete the designated interface, delete the designated interface's data set from the policy server.
Can not delete min_rate and max_rate because premium is already defined.	The maximum band restriction or the minimum band assurance cannot be deleted because the important packet flow detecting conditions (premium) have been defined. Input all the detecting conditions again to delete the maximum band restriction or the minimum band assurance.
Can not delete policy_group configuration referred by flow filter configuration.	The specified policy group cannot be deleted because the policy group name specified in the flow filer has already been set. To delete the specified policy group, it is necessary to delete the policy group name specified in the flow filter.
Can not delete replace_tos or replace_dscp because penalty_tos or penalty_dscp is already defined.	The tos rewriting value cannot be set because the contract band breaching tos rewriting value has been defined. To set the tos rewriting value, delete the contract band breaching tos rewriting value.
Can not delete tos_map or dscp_map because penalty_tos or penalty_dscp is already defined.	Tos_map cannot be set because the contract band breaching tos rewriting value has been defined. To set tos_map, delete the contract band breaching tos rewriting value.
Can not delete upc or min_rate because penalty_discard is defined.	The band setting cannot be deleted because the contract band breaching queuing priority has been defined. Delete the contract band breaching queuing priority, and then delete the band setting.
Can not delete upc because penalty_drop is defined.	The band setting cannot be deleted because the contract band breaching packet discard has been defined. Delete the contract band breaching packet discard, and then delete the band setting.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not delete upc or min_rate because penalty_tos or penalty_dscp is defined.	The band setting cannot be deleted because the contract band breaching tos rewriting value has been defined. Delete the contract band breaching tos rewriting value, and then delete the band setting.
Can not delete upc or min_rate because penalty_dscp is defined.	The band setting or minimum band guarantee cannot be deleted because the contract band breaching dscp rewriting value has been defined. Delete the contract band breaching dscp rewriting value, and then delete the band setting or minimum band guarantee. The band setting cannot be deleted because the contract band breaching dscp rewriting value has been defined. Delete the contract band breaching dscp rewriting value, and then delete the band setting.
Can not set disable.	Disable cannot be set simultaneously as changing the action. To change the disable, remove the specification of the action.
Can not set discard because replace_tos or replace_dscp is already defined.	Queuing priority cannot be set because the tos or dscp rewriting value has been defined. To set the queuing priority, delete the tos or dscp rewriting value.
Can not set discard because tos_map or dscp_map is already defined.	Queuing priority cannot be set because tos_map or dscp_map has been defined. To set the queuing priority, delete tos_map or dscp_map.
Can not set dscp_map because replace_user_priority is already defined.	It is not possible to set dscp_map because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set dscp_map.
Can not set filter_list because flow configuration is already defined.	The filter_list cannot be set because the flow filter has already been set. To set the filter, it is necessary to delete the flow filter.
Can not set flow configuration for rmEternet.	The flow interface cannot be set in the interface of rmEthernet. Set other interface name.
Can not set flow filter action because scan_extension is already defined.	An S/W search flag cannot be set simultaneously with parameters other than forward or drop. {ROUTE-OS6}
Can not set icmp protocol.	In specifying the high-order protocol, 1(icmp) cannot be specified. Specify the "icmp" by using the packet flow detecting conditions.
Can not set icmp6 protocol.	58(imp6) cannot be specified in specifying the high-order protocols. Specify "icmp6" under the packet flow detecting conditions.
Can not set igmp protocol.	In specifying the high-order protocol, 2(igmp) cannot be specified. Specify the "igmp" by using the packet flow detecting conditions.
Can not set index because replace_user_priority is already defined.	It is not possible to set the connection branch index number because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set the connection branch index number.
Can not set IPv4 IP_Address.	IPv4 addresses cannot be specified in the range of list numbers from 40001 to 60000 in the flow filter. Specify the IPv4 addresses in the range of list numbers from 1 to 20000.
Can not set IPv4 tos.	Tos rewriting value cannot be specified in the entry of IPv6 flow information.
Can not set IPv6 class.	Traffic class cannot be specified in the range of list numbers from 1 to 20000 in the flow filter. Specify the traffic class in the range of list numbers from 40001 to 60000.
Can not set IPv6 IP_Address.	IPv6 addresses cannot be specified in the range of list numbers from 1 to 20000 in the IP flow information. Specify the IPv6 addresses in the range of list numbers from 40001 to 60000.
Can not set IPv6 option header protocol.	The protocol numbers showing the IPv6 option headers (0, 43, 44, 50, 51,59, 60) cannot be specified in specifying the high-order protocols. Specify the numbers for other protocols.
Can not set max_rate because max_rate is smaller than min_rate.	The maximum band restriction cannot be set because the maximum band restriction value is smaller than that of the minimum band assurance. To set the maximum band restriction, specify a value bigger than the minimum band assurance.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set max_rate because replace_user_priority is already defined.	It is not possible to set the maximum bandwidth limitation because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set the maximum bandwidth limitation.
Can not set penalty_tos or penalty_dscp because upc or min_rate not specified.	The maximum band restriction cannot be set because the band setting has been defined. To set the Max_rate, delete the band setting.
Can not set max_rate_burst because max_rate not specified.	The maximum band restriction burst size cannot be set because the maximum band restriction has not been defined. To set the maximum band restriction burst size, set the maximum band restriction.
Can not set min_rate because min_rate is bigger than max_rate.	The minimum band assurance cannot be set because the minimum band assurance value is bigger than that of the maximum band restriction. To set the minimum band assurance, specify a value smaller than the maximum band restriction.
Can not set min_rate because replace_user_priority is already defined.	It is not possible to set the minimum bandwidth limitation because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set the minimum bandwidth limitation.
Can not set min_rate because upc is already defined.	The minimum band assurance cannot be set because the band setting has been defined. To set the Min_rate, delete the band setting.
Can not set max_rate because upc is already defined.	The maximum band assurance cannot be set because the band setting has been defined. To set the Max_rate, delete the band setting.
Can not set min_rate_burst because min_rate not specified.	The minimum band assurance burst size cannot be set because the minimum band assurance has not been defined. To set the minimum band assurance burst size, set the minimum band assurance.
Can not set penalty_discard because replace_exp is already defined.	Contract band breaching queuing priority cannot be set because the exp field rewriting value has been defined. To set the contract band breaching queuing priority, delete the exp field rewriting value.
Can not set penalty_discard because replace_tos or replace_dscp is already defined.	Contract band breaching queuing priority cannot be set because the tos or dscp rewriting value has been defined. To set the contract band breaching queuing priority, delete the tos or dscp rewriting value.
Can not set penalty_discard because replace_tos or replace_dscp or tos_map or dscp_map or replace_exp is already defined.	Contract band breaching queuing priority cannot be set because the tos or dscp rewriting value or tos_map or dscp_map, exp field rewriting value has been defined. To set the contract band breaching queuing priority, delete the tos or dscp rewriting value, or tos_map or dscp_map, exp field rewriting value.
Can not set penalty_discard because replace_user_priority is already defined.	It is not possible to set queuing priority at the time of contract bandwidth violation because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set queuing priority at the time of contract bandwidth violation.
Can not set penalty_discard because tos_map or dscp_map is already defined.	Contract band breaching queuing priority cannot be set because tos_map or dscp_map has been defined. To set the contract band breaching queuing priority, delete tos_map or dscp_map. Contract band breaching queuing priority cannot be set because the tos_map or dscp_map has been defined. To set the contract band breaching queuing priority, delete the tos_map or dscp_map.
Can not set penalty_discard because upc or min_rate not specified.	The contract band breaching queuing priority cannot be set because the band setting or the minimum band assurance has not been defined. To set the contract band breaching queuing priority, set the band setting or the minimum band assurance.
Can not set penalty_drop because replace_exp is already defined.	Contract band breaching packet discard cannot be set because the exp field rewriting value has been defined. To set the contract band breaching packet discard, delete the exp field rewriting value.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set penalty_drop because replace_user_priority is already defined.	It is not possible to set discard at the time of contract bandwidth violation because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set discard at the time of contract bandwidth violation.
Can not set penalty_drop because upc or min_rate not specified.	The contract band breaching packet discard cannot be set because the band setting or the minimum band assurance has not been defined. To set the contract band breaching packet discard, set the band setting or the minimum band assurance.
Can not set penalty_dscp because replace_user_priority is already defined.	It is not possible to set the contract bandwidth violation dscp rewrite value because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set the contract bandwidth violation dscp rewrite value.
Can not set penalty_tos or penalty_dscp because replace_user_priority is already defined.	It is not possible to set the contract bandwidth violation tos rewrite value or the contract bandwidth violation dscp rewrite value because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set the contract bandwidth violation tos rewrite value or the contract bandwidth violation dscp rewrite value.
Can not set penalty_tos or penalty_dscp because priority or discard is already defined.	Contract band breaching tos rewriting value or contract band breaching dscp rewriting value cannot be set because the output priority or queuing priority has been defined. To set the contract band breaching tos rewriting value or contract band breaching dscp rewriting value, delete output priority or queuing priority.
Can not set penalty_tos or penalty_dscp because replace_exp is already defined.	Contract band breaching tos rewriting value or contract band breaching dscp rewriting value cannot be set because the exp field rewrite value has been defined. To set the contract band breaching tos rewriting value or contract band breaching dscp rewriting value, delete exp field rewrite value.
Can not set penalty_tos or penalty_dscp because replace_tos or replace_dscp or tos_map or dscp_map is already defined.	Contract band breaching tos rewriting value or contract band breaching dscp rewriting value cannot be set because tos rewrite value, dscp rewrite value, tos_map or dscp_map. To set the contract band breaching tos rewriting value or contract band breaching dscp rewriting value, delete tos rewrite value, dscp rewrite value, tos_map or dscp_map.
Can not set penalty_tos or penalty_dscp because replace_tos or replace_dscp or tos_map or dscp_map not specified.	Contract band breaching tos rewriting value or contract band breaching dscp rewriting value cannot be set because the tos rewrite value, dscp rewrite value tos_map or dscp_map has been defined. To set the contract band breaching tos rewriting value or contract band breaching dscp rewriting value, delete tos rewrite value, dscp rewrite value tos_map or dscp_map.
Can not set priority because replace_tos or replace_dscp is already defined.	Contract band breaching queuing priority cannot be set because tos rewrite value or dscp rewrite value has been defined. To set the output priority, delete tos rewrite value or dscp rewrite value.
Can not set priority because tos_map or dscp_map is already defined.	Contract band breaching queuing priority cannot be set because tos_map or dscp_map has been defined. To set the output priority, delete tos_map or dscp_map.
Can not set qos_ip_list because flow configuration is already defined.	qos_ip_list cannot be set because flow qos has been defined. To set qos_ip_list, delete flow qos.
Can not set qos_ip_list or filter_list because flow configuration is already defined.	qos_ip_list or filter_list cannot be set because flow filter has been defined. To set qos_ip_list or filter_list, delete flow filter.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set repalce_exp and these parametors(replace_tos, replace_dscp, tos_map, dscp_map, penalty_drop, penalty_tos, penalty_dscp, penalty_discard) in the same flow list configuration.	The exp rewritten value cannot be set because any one of the tos rewritten value, dscp rewritten value, tos_map, dscp_map, contract band breach packet abortion, contract band breach queuing priority, contract band breach tos rewritten value, and contract band breach dscp rewritten value is specified simultaneously. To set the exp field rewritten value, do not specify it simultaneously with the tos rewritten value, dscp rewritten value, tos_map, dscp_map, contract band breach packet abortion, contract band breach queuing priority, contract band breach tos rewritten value, and contract band breach dscp rewritten value.
Can not set replace_exp because penalty_discard is already defined.	Exp field rewrite value cannot be set because the contract band breaching queuing priority been defined. To set the exp field rewrite value, delete contract band breaching queuing priority.
Can not set replace_exp because penalty_drop is already defined.	The exp field rewriting value cannot be deleted because the contract band breaching packet discard has been defined. To set the exp field rewriting value, delete the contract band breaching packet discard.
Can not set replace_exp because replace_tos or replace_dscp is already defined.	Exp field rewrite value cannot be set because tos rewriting value or dscp rewriting value has been defined. To set the exp field rewrite value, delete tos rewriting value or dscp rewriting value.
Can not set replace_exp because replace_user_priority is already defined.	Exp field rewrite value cannot be set because VLAN priority rewriting value has been defined. To set the exp field rewrite value, delete VLAN priority rewriting value.
Can not set replace_exp because tos_map or dscp_map is already defined.	Exp field rewrite value cannot be set because tos_map or dscp_map has been defined. To set the exp field rewrite value, delete tos_map or dscp_map.
Can not set replace_tos or replace_dscp because priority or discard is already defined.	Tos rewrite value or dscp rewrite value cannot be set because the output priority or queuing priority has been defined. To set the tos rewrite value or dscp rewrite value, delete the output priority or queuing priority.
Can not set replace_tos or replace_dscp because replace_exp is already defined.	Tos rewrite value or dscp rewrite value cannot be set because the exp field rewrite value has been defined. To set the tos rewrite value or dscp rewrite value, delete the exp field rewrite value.
Can not set replace_tos or replace_dscp because tos_map or dscp_map is already defined.	Tos rewrite value or dscp rewrite value cannot be set because tos_map or dscp_map has been defined. To set the tos rewrite value or dscp rewrite value, delete tos_map or dscp_map.
Can not set replace_user_priority.	It is not possible to specify "user_priority" except in interfaces set by InBound or VLAN.
Can not set replace_user_priority because dscp_map is already defined.	It is not possible to set the VLAN priority rewrite value because "dscp_map" is defined. Delete "dscp_map" in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because group is already defined.	It is not possible to set the VLAN priority rewrite value because the QoS group bandwidth control group number (group) is defined. Delete the QoS group bandwidth control group number (group) in order to set the VLAN priority rewrite value. [Route-OS6B]
Can not set replace_user_priority because index is already defined.	It is not possible to set the VLAN priority rewrite value because the connection branch index number is defined. Delete the connection branch index number in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because penalty_discard is already defined.	It is not possible to set the VLAN priority rewrite value because queuing priority at the time of contract bandwidth violation is defined. Delete queuing priority at the time of contract bandwidth violation in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because penalty_drop is already defined.	It is not possible to set the VLAN priority rewrite value because discard at the time of contract bandwidth violation is defined. Delete discard at the time of contract bandwidth violation in order to set the VLAN priority rewrite value.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set replace_user_priority because penalty_dscp is already defined.	It is not possible to set the VLAN priority rewrite value because the contract bandwidth violation dscp rewrite value is defined. Delete the contract bandwidth violation dscp rewrite value in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because penalty_tos or penalty_dscp is already defined.	It is not possible to set the VLAN priority rewrite value because the contract bandwidth violation tos rewrite value or the contract bandwidth violation dscp rewrite value is defined. Delete the contract bandwidth violation tos rewrite value or the contract bandwidth violation dscp rewrite value in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because replace_exp is already defined.	It is not possible to set the VLAN priority rewrite value because the exp field rewrite value is defined. Delete the exp field rewrite value in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because tos_map or dscp_map is already defined.	It is not possible to set the VLAN priority rewrite value because "tos_map" or "dscp_map" is defined. Delete "tos_map" or "dscp_map" in order to set the VLAN priority rewrite value.
Can not set replace_user_priority because upc or min_rate or max_rate is already defined.	It is not possible to set the VLAN priority rewrite value because bandwidth setting or minimum bandwidth guarantee and maximum bandwidth limit are defined. Delete bandwidth setting or minimum bandwidth guarantee and maximum bandwidth limit in order to set the VLAN priority rewrite value.
Can not set same min_rate and max_rate value in one flow list configuration.	No setting is possible because the minimum band assurance value is greater than or equivalent to that of the maximum band restriction. For the minimum band assurance, specify a value smaller than the maximum band restriction.
Can not set scan_extension.	In a flow filter, an S/W search flag cannot be set when the list number is in the range of 1 to 20000. Specify the S/W search flag when the list number is in the range of 40001 to 60000.
Can not set scan_extension because forward or drop not specified.	An S/W search flag cannot be set simultaneously with parameters other than forward or drop.
Can not set scan_extension because protocol ip not specified.	An S/W search flag cannot be set because ip is not specified in the upper protocol. To set an S/W search flag, specify ip in the upper protocol.
Can not set tcp protocol.	In specifying the high-order protocol, 6(tcp) cannot be specified. Specify the “tcp” by using the packet flow detecting conditions.
Can not set these parametors(replace_tos, replace_dscp, tos_map, dscp_map, replace_exp) in the same flow list configuration.	The tos rewriting value, dscp rewriting value, and tos_map, dscp_map, and exp field rewriting values cannot be set simultaneously. Specify them individually.
Can not set tos_map or dscp_map because priority or discard is already defined.	tos_map or dscp_map cannot be set because the output priority or queuing priority has been defined. To set the tos_map or dscp_map, delete the output priority or queuing priority.
Can not set tos_map or dscp_map because replace_exp is already defined.	tos_map or dscp_map cannot be set because the exp field rewrite value has been defined. To set the tos_map or dscp_map, delete the exp field rewrite value.
Can not set tos_map or dscp_map because replace_tos or replace_dscp is already defined.	tos_map or dscp_map cannot be set because the tos rewriting value or dscp rewriting value has been defined. To set the tos_map or dscp_map, delete the tos rewriting value or dscp rewriting value.
Can not set tos_map or dscp_map because replace_user_priority is already defined.	It is not possible to set "tos_map" or "dscp_map" because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set "tos_map" or "dscp_map".
Can not set udp protocol.	In specifying the high-order protocol, 17(udp) cannot be specified. Specify the “udp” by using the packet flow detecting conditions.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set upc because max_rate or min_rate is already defined.	The band setting cannot be set because the maximum band restriction or the minimum band assurance has been defined. To set the band setting, delete the maximum band restriction or the minimum band assurance.
Can not set upc because replace_user_priority is already defined.	It is not possible to set the bandwidth setting because the VLAN priority rewrite value is defined. Delete the VLAN priority rewrite value in order to set the bandwidth setting.
Can not set upc_burst because upc not specified.	The burst size cannot be set because the band setting has not been defined. To set Upc_burst, set the band setting.
Can not set user_priority.	It is not possible to specify "replace_user_priority" except in interfaces set by OutBound or VLAN.
class out of range	The input value is outside the specified range. Set the traffic class in the range of 0 to 255.
discard out of range	The input value is outside the specified range. Set the queuing priority in the range of 1 to 4.
Duplicate flow interface configuration.	Interface names are duplicated. Specify an interface using "<Interface_Name> + in" as one, and interfaces duplicated either in Filter or Qos cannot be specified.
Duplicate flow list No configuration.	List numbers are duplicated in the interface. Specify for the list number the numbers not having been set.
entry_no in not in range of 1 to 20000.	The input value is outside the specified range. Set the list number in the range of 1 to 20000.
exp out of range	The input value is outside the specified range. Set the exp field value in the range of 0 to 7.
Filter configuration is already defined.	The flow filter cannot be set because filter has already been set. To set the flow filter, it is necessary to delete the setting of filter_in.
Flow list IP_Address high is less then list IP_Address.	The IP address (high) is smaller in value than the IP address (low). Perform the setting so that the IP address (high) is greater in value than the IP address (low).
Flow list Port_No high is less then list Port_No low.	The port number (high) is smaller in value than the port number (low). Perform the setting so that the port number (high) is greater in value than the port number (low).
icmp_code out of range	The input value is outside the specified range. Set the ICMP code in the range of 0 to 255.
icmp_type out of range	The input value is outside the specified range. Set the ICMP type in the range of 0 to 255.
icmp6_code out of range	The input value is outside the specified range. Set the ICMP6 code in the range of 0 to 255.
icmp6_type out of range	The input value is outside the specified range. Set the ICMP6 code in the range of 0 to 255.
In case of inbound can not set replace_user_priority.	It is not possible to specify "replace_user_priority" in InBound of flow qos. Specify "replace_user_priority" in OutBound.
In case of inbound can not set vlan at VLAN interface.	It is not possible to specify "vlan" in InBound of flow filter. Specify "vlan" in OutBound.
In case of outbound can not set policy routing.	Policy, Policy_Group, and Policy_MPLS cannot be specified in OutBound of the flow filter. Specify the Policy, Policy_Group, and Policy_MPLS in the InBound
In case of outbound can not set user_priority.	It is not possible to specify "user_priority" in OutBound of flow qos. Specify "user_priority" in InBound.
index out of range	The input value is outside the specified range. Set the connection branching index number in the range of 0 to 7.
invalid IP_Address	The ip address value is invalid.
invalid IPv6_Address	The IPv6 address value is invalid.
list no. in not in range of 1 to 20000, 40001 to 60000.	The input value is outside the specified range. Set the list number in the range of 1 to 20000 or 40001 to 60000.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

lower out of range	The input value is outside the specified range. Set the lower limit of IP user data length in the range of 0 to 65535.
Masklen is not in range of 0 to 32.	The input value is outside the specified range. Set the mask length in the range of 0 to 32.
max_rate is not in range of 0 to 2400000.	The input value is outside the specified range. Set the maximum band restriction in the range of 0 to 2400000.
max_rate_burst is not in range of 0 to 131072.	The input value is out of the prescribed range. Set the range of 0 to 131072 to the maximum band limitation burst size.
Maximum number of Flow IPv6 Filter_interface configurations are already defined.	The number of entries in an interface, including a flow IPv6 filter list, which can be set per router exceeds the range. Set the interface, including a flow IPv6 filter list, to within 128 entries per router.
Maximum number of Flow IPv6 Filter_list configurations are already defined in one Flow Filter_inteface configuration.	The number of entries in a flow IPv6 filter that can be set per interface exceeds the range. Set the flow IPv6 filter to within 16 entries per interface.
Maximum number of Flow IPv6 Filter_list configurations are already defined.	The number of entry for the flow IPv6 filter that can be set per device has exceeded the range.
Maximum number of Qos/Filter IP Flow configurations are already defined.	The number of entries in a flow QoS/Filter that can be set per interface or router, exceeds the range. Set the flow QoS/Filter to within 2000 entries per RP or 10000 entries per router.
min_rate is not in range of 0 to 2400000.	The input value is out of the prescribed range. Set the range of 0 to 2400000 to the minimum band guarantee.
min_rate or max_rate not specified.	The detection conditions of an important packet flow are set, but the maximum band limitation or minimum band guarantee is not set. Set the maximum band limitation or minimum band guarantee.
min_rate_burst is not in range of 0 to 131072.	The input value is out of the prescribed range. Set the range of 0 to 131072 to the minimum band guarantee burst size.
No enough parameters.	Parameters are insufficient. Specify the necessary parameters.
no such flow	Applicable flow configuration definition does not exist.
No such flow filter list No.	The specified list number does not exist because the action of a flow filter was changed. Specify the previously set list number when action was changed.
No such flow qos list No.	The specified list number does not exist because the action of a flow qos was changed. Specify the previously set list number when action was changed.
penalty_discard out of range	The input value is out of the prescribed range. Set the range of 1 to 4 to delete contract band breaching queuing priority.
penalty_tos out of range	The input value is out of the prescribed range. Set the range of 0 to 255 to delete contract band breaching tos rewrite value.
Policy interface name can not set at rmEthernet.	The interface for the policy routing cannot be set in the interface of mEthernet. Set other interface name.
Policy interface name not found at [<Interface_Name>]	The interface specified in the policy routing cannot be found. Set the interface name.
Policy_group name not found at [<Policy_Group_Name>].	The specified in the policy group cannot be found. Set either the policy routing or the policy group set in the policy routing.
port_destination out of range	The input value is out of the prescribed range. Set the range of 1 to 65535 to the destination port number.
port_source out of range	The input value is out of the prescribed range. Set the range of 1 to 65535 to the source port number.
precedence out of range	The input value is out of the prescribed range. Set the range of 0 to 7 to the precedence value.
prefixlen out of range	The input value is out of the prescribed range. Set the range of 0 to 128 to the prefix length.
priority out of range	The input value is out of the prescribed range. Set the range of 1 to 1000 to the output priority.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

protocol out of range	The input value is out of the prescribed range. Set the range of 1 to 255 to the protocol number.
QoS IP configuration is already defined.	flow qos cannot be set because qos_ip has been set. To set flow qos, delete qos_ip.
Relation between regular protocol and premium protocol are inconsistent.	The relation between the protocol of normal packet flow detecting condition and the protocol of important packet flow detecting condition is in disagreement. Make the protocol of normal packet flow detecting condition an “IP” or have the both protocols agree with each other.
replace_exp out of range	The input value is out of the prescribed range. Set the range of 0 to 7 to the exp field rewrite value.
replace_tos out of range	The input value is out of the prescribed range. Set the range of 0 to 255 to the tos rewrite value.
replace_user_priority out of range	The input value is out of the prescribed range. Set the range of 0 to 7 to the VLAN priority rewriting value.
tos out of range	The input value is out of the prescribed range. Set the range of 0 to 255 to the tos.
upc bandwidth is not in range of 0 to 2400000.	The input value is out of the prescribed range. Set the range of 0 to 2400000 to the bandwidth.
upc_burst is not in range of 0 to 131072.	The input value is out of the prescribed range. Set the range of 0 to 131072 to the burst size.
upper out of range	The input value is out of the prescribed range. Set the range of 0 to 65535 to the upper value of IP user data length.
user_priority out of range	The input value is out of the prescribed range. Set the range of 0 to 7 to the VLAN priority value.
vlan out of range	The input value is out of the prescribed range. Set the range of 1 to 4095 to vlan.
Can not set replace_tos or replace_dscp because penalty_discard is already defined.	Tos rewrite value or dscp rewrite value cannot be set because the contract band breaching queuing value has been defined. To set the contract band breaching queuing value, delete tos rewrite value or dscp rewrite value.
Can not set tos_map or dscp_map because penalty_discard is already defined.	Tos_map or dscp_map cannot be set because the contract band breaching queuing value has been defined. To set the contract band breaching queuing value, delete tos_map or dscp_map.
replace_dscp out of range	The input value is out of the prescribed range. Set the range of 0 to 63 to the dscp rewrite value.
penalty_dscp out of range	The input value is out of the prescribed range. Set the range of 0 to 63 to the contract band breaching dscp rewrite value.
dscp out of range	The input value is out of the prescribed range. Set the range of 0 to 63 to the dscp value.
Can not set IPv4 tos and exp.	Tos value and exp field value cannot be specified in the entry of the IPv6 flow information.
Can not set IPv4 exp.	Exp field value cannot be specified in the entry of the IPv6 flow information.
Can not set IPv4 replace_exp.	Exp field value cannot be specified in the entry of the IPv6 flow information.
Can not set IPv4 tos_map.	tos_map cannot be specified in the entry of the IPv6 flow information.
Can not set IPv4 replace_tos.	Tos rewrite value cannot be specified in the entry of the IPv6 flow information.
Can not set IPv4 penalty_tos.	Contract band breaching tos rewrite value cannot be specified in the entry of the IPv6 flow information.
Can not set IPv4 tos_map and penalty_tos.	Contract band breaching tos rewrite value and tos_map cannot be specified in the entry of the IPv6 flow information.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set penalty_dscp because upc or min_rate not specified.	Contract band breaching dscp rewrite value cannot be set because the band setting or the minimum band assurance has not been defined. To set the contract band breaching dscp rewrite value, define the band setting or the minimum band assurance.
Can not set these parametors(replace_dscp, dscp_map) in the same flow list configuration.	The dscp rewrite value and the dscp_map cannot be set simultaneously. Specify the respective settings individually.
Can not set penalty_discard because replace_dscp is already defined.	Contract band breaching queuing priority cannot be set because the dscp rewrite value has been defined. To set the contract band breaching queuing priority, delete the dscp rewrite value.
Can not set penalty_discard because dscp_map is already defined.	Contract band breaching queuing priority cannot be set because dscp_map has been defined. To set the contract band breaching queuing priority, delete the dscp_map.
Can not set priority because replace_dscp is already defined.	Output priority cannot be set because the dscp rewrite value has been defined. To set the output priority, delete the dscp rewrite value.
Can not set priority because dscp_map is already defined.	Output priority cannot be set because dscp_map has been defined. To set the output priority, delete the dscp_map.
Can not set discard because replace_dscp is already defined.	Queuing priority cannot be set because the dscp rewrite value has been defined. To set the queuing priority, delete the dscp rewrite value.
Can not set discard because dscp_map is already defined.	Queuing priority cannot be set because dscp_map has been defined. To set the queuing priority, delete dscp_map.
Can not set replace_dscp because priority or discard is already defined.	The contract band breaching dscp rewrite value cannot be set because the output priority or queuing priority has been defined. To set the contract band breaching dscp rewrite value, delete the output priority or queuing priority.
Can not set replace_dscp because dscp_map is already defined.	The dscp rewrite value cannot be set because the output priority or queuing priority has been defined. To set the dscp rewrite value, delete the output priority or queuing priority.
Can not set replace_dscp because penalty_discard is already defined.	The dscp rewrite value cannot be set because the contract band breaching queuing priority has been defined. To set the dscp rewrite value, delete the contract band breaching queuing priority.
Can not set penalty_dscp because priority or discard is already defined.	The contract band breaching dscp rewrite value cannot be set because the output priority or queuing priority has been defined. To set the contract band breaching dscp rewrite value, delete the output priority or queuing priority.
Can not set penalty_dscp because replace_dscp or dscp_map not specified.	The contract band breaching dscp rewrite value cannot be set because the dscp rewrite value or dscp_map has been defined. To set the contract band breaching dscp rewrite value, delete the dscp rewrite value or dscp_map.
Can not set dscp_map because priority or discard is already defined.	The dscp_map cannot be set because the output priority or queuing priority has been defined. To set dscp_map rewrite value, delete the output priority or queuing priority.
Can not set dscp_map because replace_dscp is already defined.	The dscp_map cannot be set because the dscp rewrite value has been defined. To set dscp_map rewrite value, delete the dscp rewrite value.
Can not set dscp_map because penalty_discard is already defined.	The dscp_map cannot be set because the contract band breaching queuing priority has not been defined. To set contract band breaching queuing priority rewrite value, delete dscp_map.
Can not set penalty_dscp because upc or min_rate not specified.	Contract band breaching dscp rewrite value cannot be set because the band setting or the minimum band assurance has not been defined. To set the contract band breaching dscp rewrite value, define the band setting or the minimum band assurance.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set penalty_discard because replace_dscp or dscp_map is already defined.	Contract band breaching queuing priority cannot be set because the dscp rewrite value or dscp_map has been defined. To set the contract band breaching queuing priority, delete the dscp rewrite value or dscp_map.
Can not set penalty_dscp because replace_dscp or dscp_map is already defined.	Can not set penalty_dscp because replace_dscp or dscp_map is already defined.
Can not delete replace_dscp because penalty_dscp is already defined.	The dscp rewrite value cannot be set because the contract band breaching dscp rewrite value has been defined. To set the dscp rewrite value, delete the contract band breaching dscp rewrite value.
Can not delete dscp_map because penalty_dscp is already defined.	The dscp_map cannot be set because the contract band breaching dscp rewrite value has been defined. To set the dscp_map, delete the contract band breaching dscp rewrite value.
Can not set or change IPv6 flow qos.	The IPv6 flow QoS information can neither be set nor changed in the RP-A1, RP-C and RP-D.
Can not set Tunnel interface in flow qos configuration.	The flow qos cannot be set in the tunnel interface.
cops_range out of range	The input value is out of the prescribed range. Set the range of 1 to 20,000 to the list number used in COPS function.
syntax error	Syntax error
Can not delete qos_interface configuration referred by flow qos configuration.	The designated qos_interface configuration definition cannot be deleted because the QoS group band control group number (group) designated by the flow qos has been set. To delete the designated qos_interface configuration definition, delete the QoS group band control number that has been designated by the flow qos. [ROUTE-OS6B]
No such QoS group number.	The QoS group band control group number (group) designated by the flow qos does not exist. Designate the QoS group band control group number that has been set. [ROUTE-OS6B]
Can not set penalty_drop because group is already defined.	Contract band breach packet abolishment cannot be set because the QoS group band control group number (group) has been defined. To set contract band breach packet abolishment, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set replace_tos or replace_dscp because group is already defined.	The rewritten values for the contract band breach tos or the contract band breach dscp cannot be set because the QoS group band control group number (group) has been defined. To set the rewritten values for contract band breach tos or contract band breach dscp, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set penalty_tos or penalty_dscp because group is already defined.	The rewritten values for the contract band breach tos or the contract band breach dscp cannot be set because the QoS group band control group number (group) has been defined. To set the rewritten values for contract band breach tos or contract band breach dscp, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set tos_map or dscp_map because group is already defined.	The tos_map or the dscp_map cannot be set because the QoS group band control group number (group) has been defined. To set the tos_map or the dscp_map, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set replace_exp because group is already defined.	The rewritten value for the exp field cannot be set because the QoS group band control group number (group) has been defined. To set the rewritten value for the exp field, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set penalty_discard because group is already defined.	The contract band breach queuing priority cannot be set because the QoS group band control group number (group) has been defined. To set the contract band breach queuing priority, delete the QoS group band control group number. [ROUTE-OS6B]

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Flow Information Error Messages (continued)

Can not set replace_dscp because group is already defined.	The rewritten value for the contract band breach dscp cannot be set because the QoS group band control group number (group) has been defined. To set rewritten value for the contract band breach dscp, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set penalty_dscp because group is already defined.	The rewritten value for the contract band breach dscp cannot be set because the QoS group band control group number (group) has been defined. To set rewritten value for the contract band breach dscp, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set dscp_map because group is already defined.	The dscp_map cannot be set because the QoS group band control group number (group) has been defined. To set the dscp_map, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set index because group is already defined.	The connection branching index number cannot be set because the QoS group band control group number (group) has been defined. To set the connection branching index number, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set upc because group is already defined.	The band setting cannot be set because the QoS group band control group number (group) has been defined. To set the band setting, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set max_rate because group is already defined.	The maximum band restriction cannot be set because the QoS group band control group number (group) has been defined. To set the maximum band restriction, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set min_rate because group is already defined.	The minimum band guarantee cannot be set because the QoS group band control group number (group) has been defined. To set the minimum band guarantee, delete the QoS group band control group number. [ROUTE-OS6B]
Can not set qos_ip_list or filter_list because nat configuration is already defined.	It is not possible to set "qos_ip_list" or "filter_list" because nat configuration information is set. It is necessary to delete nat in order to set "qos_ip_list" or "filter_list."
Can not set flow configuration,qos_ip_list or filter_list configuration simultaneously.	It is not possible to simultaneously set flow configuration information and "qos_ip_list" or "filter_list" in the configuration definition file. Delete "qos_ip_list" or "filter_list" in order to set flow configuration information. In addition, delete flow configuration information in order to set "qos_ip_list" or "filter_list."

Downloaded from www.Manualslib.com manuals search engine

5.9 Filter and QoS Information (Other than Flow Information)

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

Message	Contents
Branch index is greater than group index.	DLCI/VC selection number exceeded index value of specified group. Specify a DLCI/VC selection number not exceeding the index value of the specified group.
Can not delete filter group configuration referred by filter interface configuration.	IP filter interface information present. Delete IP filter interface information; delete IP filter group information.
Can not delete filter list configuration referred by filter group configuration.	IP filter group information present. Delete IP filter group information; delete IP filter list information.
Can not delete QoS IP list configuration referred by QoS IP list group configuration.	Attempt made to delete QoS IP list information referred by QoS IP list group. Delete QoS IP list of QoS IP list group; delete QoS IP list information.
Can not delete QoS IP list group configuration referred by QoS IP configuration.	Attempt made to delete QoS IP list information referred by QoS IP list group. Delete QoS IP list of QoS IP list group; delete QoS IP list information.
Can not delete QoS queue list configuration referred by QoS interface configuration.	Attempt made to delete QoS IP list information referred by QoS interface information. Delete QoS queue list of QoS interface information; delete QoS queue list information.
Can not delete QoS with QoS bridge configuration.	Attempt made to delete QoS, but QoS bridge information is configured. Delete QoS bridge information; delete QoS.
Can not delete QoS with QoS discard mode configuration.	Attempt made to delete QoS, but QoS discard mode information is configured. Delete QoS discard mode information; delete QoS.
Can not delete QoS with QoS HDLC configuration.	Attempt made to delete QoS, but QoS HDLC information is configured. Delete HDLC information; delete QoS.
Can not delete QoS with QoS IP configuration.	Attempt made to delete QoS, but QoS IP information is configured. Delete QoS IP information; delete QoS.
Can not delete QoS with QoS IP list configuration.	Attempt made to delete QoS, but QoS IP list information is configured. Delete QoS IP list information; delete QoS.
Can not delete QoS with QoS IPX configuration.	Attempt made to delete QoS, but QoS IPX information is configured. Delete QoS IPX information; delete QoS.
Can not delete QoS with QoS queue list configuration.	Attempt made to delete QoS, but QoS queue list information is configured. Delete QoS queue list information; delete QoS.
Can not delete QoS with QoS TOS configuration.	Attempt made to delete QoS, but QoS TOS information is configured. Delete QoS TOS information; delete QoS.
Can not delete vlan configuration referred by shaper configuration.	It is not possible to delete of specified VLAN line interfaces because the names of VLAN line interfaces specified by shaper configuration information are set. It is necessary to delete the names of VLAN line interfaces specified by shaper configuration information in order to delete VLAN line interfaces.
Can not set cops.	cops cannot be set in QoS. Delete the QoS interface information and QoS queue list information.
Can not set QoS interface configuration on interface which is not bound to any protocol.	Attempt made to set the QoS interface configuration on an interface not bound to any protocol. Set a protocol first.
Can not set QoS IP list exp.	EXP value of QoS list cannot be specified. Delete TOS modified value, EXP field modified value or QoS control switch to specify EXP value.
Can not set QoS IP list replace exp.	EXP value of QoS list cannot be specified. Delete TOS modified value, EXP field modified value or QoS control switch to specify EXP value.
Can not set QoS IP list replace tos.	TOS modified value of QoS list cannot be specified. Can not set TOS modified value, when EXP field modified value or EXP value has set yet.

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

Can not set QoS IP list tos map.	QoS control switch of QoS list cannot be specified. Can not be configured Qos control switch, when EXP field modified value or EXP value has set yet.
Can not set QoS IP list upc penalty drop.	Can not set QoS IP list upc penalty drop to discard. Can not be configured upc penalty drop to discard, when EXP field modified value or EXP value has set yet
Can not set QoS IP list upc penalty modified discard class.	Can not set QoS IP list upc penalty modified queuing priority class. Can not be configured pc penalty modified queuing priority, when EXP field modified value or EXP value has set yet
Can not set QoS IP list upc penalty modified new tos number.	Can not set QoS IP list upc penalty modified new tos number. Set IP header TOS modified value or IP header TOP QoS control switch to unused.
Can not set QoS IP list upc penalty modified priority class.	Can not set QoS IP list upc penalty modified output priority class. Can not be configured upc penalty modified output priority, when EXP field modified value or EXP value has set yet
Can not set QoS IP list upc penalty.	Can not set QoS IP list upc penalty modified output priority class. Can not be configured upc penalty modified output priority, when EXP field modified value or EXP value has set yet
Can not set QoS IP list upc.	Can not set QoS IP list upc penalty tos modified value. Can not be configured upc penalty tos modified value, when EXP field modified value or EXP value has set yet
Can not set QoS queue list traffic min rate.	The minimum queue traffic guarantee band cannot be set for the QoS IP list. To set the minimum queue traffic guarantee band, change the queue traffic category to “guarantee.”
Can not set QoS queue list traffic weight.	Weight allocation of the queue traffic excess band cannot be set for the QoS IP list. To set the weight allocation of the queue traffic excess band, change the queue traffic category to “guarantee”.
Can not set Rate.	It is not possible to specify the maximum send bandwidth value in the specified queue mode.
Can not set shaper configuration.	It is not possible to set shaper configuration information. When setting configuration information, set it in NIFs or interfaces compatible with shaper configuration information.
Cops is specified in QoS.	cops is set in QoS. Delete cops of QoS.
Duplicate filter group configuration.	The same IP filter group entry content is used. Make each IP filter group entry content unique.
Duplicate filter interface configuration.	IP filter interface entry of the same content is specified. Make each IP filter interface entry content unique.
Duplicate filter list configuration.	IP filter list of the same content is used. Make each IP filter list content unique.
Duplicate QoS IP list group configuration.	QoS IP group of the same content is specified. Make each entry content unique.
Duplicate shaper configuration.	Interface names are duplicated in shaper configuration information. Specify interface names that have not already been set.
Filter group name not specified.	Group name of the IP filter group entry has not been specified. Specify a group name.
Filter group not specified.	IP filter group has not been specified. Specify an IP filter group.
Filter group number not specified.	Filtering list entry number of IP filter group entry has not been specified. Specify an entry number of the filter list.
Filter interface group name not specified.	IP filter interface group name has not been specified. Specify a group name.
Filter interface name not specified.	IP filter interface name has not been specified. Specify an interface name.
Filter interface not specified.	For IP filter setting, IP filter interface entry has not been specified. Specify an IP filter interface entry, then set the IP filter use switch to “yes.”

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

Filter list not specified.	IP filter list has not been specified. Specify an IP filter list.
Filter list number not specified.	IP filter list entry number has not been specified. Specify the entry number.
Filter not specified.	IP filter has not been specified. Specify the IP filter.
Invalid ip destination network class.	Invalid ip destination network class and sub-network class. Specify ip destination network class and sub-network class.
Invalid ip source network class.	Invalid ip source network class and sub-network class. Specify ip source network class and sub-network class.
Invalid name <name>.	Entered name of configuration information invalid. For interface: Specify interface except for AUX name on IP defined. For Qos IP, Qos IPX, Qos bridge, QoS HDLC: Specify interface except for rmEthernet and AUX name on IP defined For QoS interface: Specify name set in ethernet, frame relay, dlci, ppp and isdn ppp.
	A name of <name> configuration information.
Invalid phb scheduling class.	Invalid band configuration value. Specify band configuration value when band configuration type is cs or af.
Invalid policy routing group name.	Invalid policy routing group name. Specify policy routing group name.
Invalid policy routing interface name.	Invalid policy routing interface name. Specify policy routing interface name in except for AUX.
Invalid QoS discard mode NIF no.	This is NIF number of ATM. Specify NIF number of NIF other than the already set ATM.
Invalid QoS interface name.	ATM line, timeslot or line where Frame-Relay protocol operates is specified. Specify an interface name of an interface except an ATM line, timeslot or line where Frame Relay protocol operates is specified.
invalid Rate4	The maximum send bandwidth of queue #4 is invalid.
IP destination high is less than IP destination low.	Destination IP address (high) is less than destination IP address (low). Specify a destination IP address (high) greater than the destination IP address (low).
IP source high is less than IP source low.	Source IP address (high) is less than source IP address (low). Specify a source IP address (high) greater than source IP address (low).
length out of range	The input value exceeds the prescribed range. Set the queue length within the range of 0 - 4000.
Maximum number of filter group configurations area already defined.	Number of the IP filter group entries exceeded 256. Decrease the entries to 256 or fewer.
Maximum number of filter list configurations are already defined.	No more IP filter list configurations can be defined. Decrease the list configurations to no more than the total of 1024 entries including the QoS IP list configurations.
Maximum number of QoS bridge configurations are already defined on the RP.	Maximum number of QoS bridge configurations are already defined on the RP. Set to 32 or less configuration per RP.
Maximum number of QoS bridge configurations are already defined.	Maximum number of QoS bridge configurations are already defined. Set to 5 or less information per RP.
Maximum number of QoS hdlc passthrough configurations are already defined on the RP.	Maximum number of QoS hdlc passthrough configurations are already defined on the RP. Set to 32 or less information per RP..
Maximum number of QoS hdlc passthrough configurations are already defined.	Maximum number of QoS hdlc passthrough configurations are already defined. Set to 5 or less information per RP.
Maximum number of QoS interface configurations are already defined on the RP.	Maximum number of Qos interface configurations already defined on RP. The limit is 480 entries per RP.
Maximum number of QoS IP configurations are already defined on the RP.	Number of QoS IP configurations exceeded maximum value. Decrease number to 512 per RP.
Maximum number of QoS IP list configurations are already defined.	No more QoS IP list configurations can be defined. Decrease list configurations to no more than a total of 1024 entries including IP filter list configurations.

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

Maximum number of QoS IP list group configurations are already defined.	Maximum number of QoS IP group configurations are already defined. Decrease group configuration to 256 entries or fewer.
Maximum number of QoS IPX configurations already defined on the RP.	The maximum number of QoS IPX information per RP has already been set. Specify QoS IPX information in 32 types or less per RP.
Maximum number of QoS IPX configurations already defined.	Maximum number of QoS IPX configurations are already defined. Allowed configuration number of QoS IPX information are up to 5RPs.
No such filter group name.	Group name of the IP filter interface has not been specified. Specify the group name of the specified filter group.
No such filter interface in/out flag.	Inbound/Outbound flag has not set. Specify Inbound/Outbound flag.
No such filter list number.	Filter list specified with IP filter group entry has not been specified. Specify an entry number in the specified filter list.
No such insert index.	An entry cannot be inserted on specified entry number. Use entry number not exceeding the number of set entries.
No such name <name>.	Specified configuration information name not found. Specify existing definition information name.
	A name of <name> configuration information.
No such QoS discard mode NIF number.	There is no such QoS discard mode NIF number. Specify NIF number of NIF other than the already set ATM.
No such QoS interface name.	No such interface specified for QoS interface. Specify interface name of an interface except the already set ATM line.
No such QoS interface queue list name.	There is no such QoS queue list name specified in QoS interface. Specify the QoS queue list name for the QoS queue list.
No such QoS IP list group entry number.	There is no such QoS IP group entry number. Specify entry number of an already specified IP list.
No such QoS IP list group name.	There is no such IP group specified in QoS IP. Specify group name of already set IP group.
No such set index.	An entry cannot be set on specified entry number. Use entry number not exceeding the set number of entries. To add entries, use the number of set entries +1 for entry value.
No such shaper configuration.	There is no specified shaper configuration information. Confirm the specified shaper configuration information.
Payload length not specified.	IP user data length has not been specified. Specify an IP user data length or delete specification of IP user data upper limit/lower limit.
peak_rate out of range	The input value exceeds the prescribed range. Set the value in the range of 500 - 980000 in maximum bandwidth if Kbit/s is specified and in the range of 1M - 980M if Mbit/s is specified.
phb scheduling class not specified.	Band configuration value has not set. Specify band configuration value when band configuration type is cs or af.
Policy routing IP address not specified.	Next hop IP address has not been specified. Specify next hop IP address or delete policy routing specification.
Port destination high is less than port destination low.	Destination port number (high) is less than destination port number (low). Specify a destination port number (high) greater than the destination port number (low).
Port source high is less than port source low.	Source port number (high) is less than source port number (low). Specify a source port number (high) greater than the source port number (low).
QoS discard mode NIF number not specified.	NIF number in QoS discard mode has not been specified. Specify an NIF number.
QoS interface name not specified.	QoS interface name has not been specified. Specify the interface name.
QoS interface queue list name not specified.	QoS interface queue list name has not been specified. Specify a QoS queue list name.
QoS IP in/out flag not specified.	QoS IP in/out flag is not specified. Specify Inbound/Outbound flag.

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

QoS IP list group entry number not specified.	QoS IP list group entry number has not been specified. Specify an IP list number.
QoS IP list group name not specified.	QoS IP group name has not been specified. Specify IP group name.
QoS IP list ip destination high is less than QoS IP list ip destination low.	Destination IP address (high) is less than the destination IP address (low). Correct the value so the destination IP address (high) becomes more than the destination IP address (low).
QoS IP list ip source high is less than QoS IP list ip source low.	Source IP address (high) is less than source IP address (low). Correct the value so the source IP address (high) becomes more than the source IP address (low).
QoS IP list not specified.	QoS IP list has not been specified. Before specifying QoS IP group, specify a QoS IP list.
QoS IP list number not specified.	QoS IP list entry number has not been specified. Specify a QoS IP list entry number.
QoS IP list payload length not specified.	QoS IP list IP user data length has not been specified. Specify IP user data length or delete specification of the IP user data length upper limit/lower limit.
QoS IP list port destination high is less than QoS IP list port destination low.	Destination port number (high) is less than the destination port number (low). Correct the value so the destination port number (high) becomes more than the destination port number (low).
QoS IP list port source high is less than QoS IP list port source low.	Source port number (high) is less than the source port number (low). Correct the value so the source port number (high) becomes more than the source port umber (low).
QoS IP list upc penalty modified discard class not specified.	QoS IP list UPC penalty modified discard class has not been specified. Specify UPC penalty modified discard class or delete definition of the UPC penalty modified delay class.
QoS IP list upc penalty modified priority class not specified.	QoS IP list UPC penalty modified priority class has not been specified. Specify UPC penalty modified priority class, or delete definition of the UPC penalty modified priority class.
QoS not specified.	QoS has not been specified. Before QoS related information, specify QoS.
QoS queue list bandwidth not specified.	QoS queue list bandwidth has not been specified. Specify one or more bandwidth values, or set the queue mode to priority.
QoS queue list name not specified.	QoS queue list name has not been specified. Specify a QoS queue list name.
QoS queue list not specified.	QoS queue list has not been specified. Before specifying a QoS interface, specify a QoS queue list.
QoS queue list traffic min rate not specified.	QoS queue list traffic min rate not specified. Specify the QoS queue list traffic min rate.
QoS queue list traffic peak rate not specified.	QoS queue list traffic peak rate not specified. Specify the QoS queue list traffic peak rate.
QoS queue list traffic type not specified.	QoS queue list traffic type not specified. Specify the QoS queue list traffic type.
rate out of range	The input value exceeds the prescribed range. Set the value in the range of 1 - 100 in maximum bandwidth.
Relations between max queue number and traffic queue number are inconsistent.	Relations between max queue number and traffic queue number are inconsistent. Set the correct value.
Relations between pair synchronized and IP pair are inconsistent.	Although the IP address/high-order protocol port pair specification is on, the IP address pair switch is on. Turn IP address/high-order protocol port pair specification or IP address pair switch off.
Relations between pair synchronized and port pair are inconsistent.	Although the IP address/high-order protocol port pair specification is on, the high-order protocol number pair switch is on. Turn IP address/high-order protocol port pair specification or high-order protocol number pair switch off.

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

Relations between QoS IP list discard class, QoS IP list replace tos and QoS IP list tos map are inconsistent.	QoS IP list discard class cannot be specified. To specify class, cancel the IP header TOS modified value or the IP header TOS QoS control switch.
Relations between QoS IP list ip pair switch and QoS IP list pair synchronized are inconsistent.	Although the IP address/high-order protocol port pair specification is on, the IP address pair switch is on. Turn IP address/high-order protocol port pair specification or IP address pair switch off.
Relations between QoS IP list port pair switch and QoS IP list pair synchronized are inconsistent.	Although the IP address/high-order protocol port pair specification is on, the high-order protocol number pair switch is on. Turn IP address/high-order protocol port pair specification off; turn the high-order protocol number pair switch off.
Relations between QoS IP list priority class, QoS IP list replace tos and QoS IP list tos map are inconsistent.	QoS IP list delay class cannot be specified. To specify class, cancel the IP header TOS modified value or the IP header TOS QoS control switch.
Relations between QoS IP list replace exp and QoS IP list exp are inconsistent.	Both the QoS IP list IP header exp modified value and the IP header exp value are set. Turn either or both off.
Relations between QoS IP list replace tos and QoS IP list exp are inconsistent.	Both the QoS IP list IP header TOS modified value and the IP header exp value are set. Turn either or both off.
Relations between QoS IP list replace tos and QoS IP list replace exp are inconsistent.	Both the QoS IP list IP header tos modified value and the IP header exp field modified value are set. Turn either or both off.
Relations between QoS IP list replace tos and QoS IP list tos map are inconsistent.	Both the QoS IP list IP header modified value and the IP header TOS QoS control switches are set. Turn either or both off.
Relations between QoS IP list tos map and QoS IP list exp are inconsistent.	Both the QoS IP list IP header TOS QoS control switches and the IP header exp value are set. Turn either or both off.
Relations between QoS IP list tos map and QoS IP list replace exp are inconsistent.	Both the QoS IP list IP header TOS QoS control switches and the IP header exp modified value are set. Turn either or both off.
Relations between QoS IP list upc penalty drop and QoS IP list upc are inconsistent.	During QoS IP list UPC penalty, operation cannot be discarded. Specify the UPC function used/unused switch and the UPC contract bandwidth.
Relations between QoS IP list upc penalty drop and QoS IP list upc penalty modified new tos number are inconsistent.	During QoS IP list UPC penalty, operation cannot be discarded. Delete specification of the UPC penalty TOS modified value.
Relations between QoS IP list upc penalty modified discard class and QoS IP list upc bandwidth are inconsistent.	QoS IP list UPC penalty discard class cannot be specified. To specify class, set UPC function used/unused switch to used and specify UPC contract bandwidth.
Relations between QoS IP list upc penalty modified discard class, QoS IP list replace tos and QoS IP list tos map are inconsistent.	Relations between QoS IP list upc penalty modified discard class, QoS IP list replace tos and QoS IP list tos map are inconsistent.
Relations between QoS IP list upc penalty modified new tos number and QoS IP list upc bandwidth are inconsistent.	During QoS IP list UPC penalty, TOS modified value cannot be specified. Delete specification of UPC penalty operation. To specify, set UPC function used/unused switch to unused, then specify UPC contract bandwidth.
Relations between QoS IP list upc penalty modified priority class, QoS IP list upc penalty modified discard class and QoS IP list upc penalty drop are inconsistent.	QoS IP list UPC penalty delay class cannot be specified. To specify class, cancel the modified output priority class and the modified queuing priority class.
Relations between QoS IP list upc penalty modified priority class and QoS IP list upc bandwidth are inconsistent.	QoS IP list UPC penalty delay class cannot be specified. To specify class, set the used/unused switch to used and specify UPC contract bandwidth.
Relations between QoS IP list upc penalty modified priority class, QoS IP list replace tos and QoS IP list tos map are inconsistent.	QoS IP list UPC penalty delay class cannot be specified. To specify class, cancel the IP header TOS modified value or IP header TOS control switch.
Relation between Rate1, Rate2 and Rate3 are inconsistent.	The sum total of the maximum send bandwidth of queues #1-3 is greater than 100%. Set the value so that the sum total does not exceed 100%.

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Filter and QoS Information (Other than Flow Information) Error Messages

Relation between Rate1, Rate2, Rate3 and Rate4 are inconsistent.	The sum total of the maximum send bandwidth of each queue is greater than 100%. Set the value so that the sum total does not exceed 100%.
The total of QoS queue list bandwidth exceeded 100%.	Total of QoS queue list bandwidth values exceeded 100%. Decrease the total to 100% or less.
The total of traffic peak rate, traffic min rate exceeded bandwidth traffic.	The sum of the queue traffic minimum guarantee band and the queue traffic maximum restriction band exceeds the band allocation control (traffic). Set it so that the value is less than the band allocation control (traffic).
Relations between traffic min rate and traffic peak rate are inconsistent.	Relations between traffic min rate and traffic peak rate are inconsistent. Set the correct value.
Relations between traffic peak rate and bandwidth traffic are inconsistent.	Relations between traffic peak rate and bandwidth traffic are inconsistent. Set the correct value.
Invalid UPC group No.	The upe group number is incorrect. Set the value correctly.
Invalid UPC mode.	The band control (max_rate_importance, max_rate_normal, min_rate_importance, min_rate_normal) has been set incorrectly. Set the value correctly.
UPC bandwidth not specified.	The contract band when the contract band surveillance function is in use has not been set. Set the contract band.
Can not set flow configuration,qos_ip_list or filter_list configuration simultaneously.	It is not possible to simultaneously set flow configuration information and "qos_ip_list" or "filter_list" in the configuration definition file. Delete "qos_ip_list" or "filter_list" in order to set flow configuration information. In addition, delete flow configuration information in order to set "qos_ip_list" or "filter_list."

Downloaded from www.Manualslib.com manuals search engine

5.10 MPLS Information

Table 5-10 MPLS Information Error Messages [ROUTE-OS7]

Message	Contents
explicit_route: duplicate IP address at '<Address>' in list '<ER name>'	IP address is duplicated.
	<Address>: Specified address <ER name>: Specified route name
explicit_route: invalid IP address '<Address>' in '<ER name>'	IP address is invalid.
	<Address>: Specified address <ER name>: Specified route name
explicit_route: invalid mask value at '<value>' in '<Address>' not in 1 to 32 in '<ER name>'	Mask value is out of range. Set the mask between 1 and 32.
	<value>: Specified mask length <Address>: Specified address <ER name>: Specified route name
explicit_route: invalid mask value '<Address>' '<Mask>' in '<ER name>'	Mask value is invalid.
	<Address>: Specified address <Mask>: Specified mask <ER name>: Specified route name
l2transport: duplicate description in '<Interface Name>'	Duplicate definitions.
	<Interface name>: interface name
l2transport: duplicate in_exp in '<Interface Name>'	Duplicate definitions.
	<Interface name>: interface name
l2transport: duplicate interface name '<Interface Name>'	Duplicate definitions.
	<Interface name>: interface name
l2transport: duplicate out_exp in '<Interface Name>'	Duplicate definitions.
	<Interface name>: interface name
l2transport: duplicate vcid '<Value>' in '<Interface Name>'	Duplicate definitions.
	<Value>: VCID value <Interface name>: interface name
l2transport: invalid replace_value value '<Value>' not in range 0 to 7	The value of "replace_value" is invalid. Set "replace_value" in the range of 0 - 7.
	<Value>: replace_value value
l2transport: invalid vcid value '<VCID>' not in range 1 to 4294967295	The value of "replace_value" is invalid. Set "replace_value" in the range of 0 - 4294967295.
	<VCID>: Specified route name
label_switched_path: duplicate explicit_route_name '<ER name>' in '<LSP name>'	This is a duplicated definition.
	<ER name>: Specified route name <LSP name>: Specified LSP name
label_switched_path: duplicate flow_map '<Address>' in '<LSP name>'	The destination IP is incorrect. The designated flow_map already has been registered.
	<Address>: Specified address <LSP name>: Specified LSP name
label_switched_path: duplicate flow_map in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
label_switched_path: duplicate pinning in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
label_switched_path: duplicate remote_vpn in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
label_switched_path: duplicate retry_interval in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
label_switched_path: duplicate secondary_label_switched_path in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name

Downloaded from www.Manualslib.com manuals search engine

Table 5-10 MPLS Information Error Messages [ROUTE-OS7] (continued)

label_switched_path: duplicate 'to <Address>' in '<LSP name>'	This is a duplicated definition of the "to parameters."
	<Address>: Specified address <LSP name>: Specified LSP name
label_switched_path: duplicate vpn in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
label_switched_path: either 'to' or explicit_route_name is needed in '<LSP name>'	Destination is unknown because "to" and the explicit_route_name has not been designated. Set at least either one of them.
	<LSP name>: Specified LSP name
label_switched_path: flow_map ip address should no be same as 'to <Address>' '<Mask>'	The IP designation is incorrect. The value designated by "to" has been designated in flow-map.
	<Address>: Specified address <Mask>: Specified mask
label_switched_path: invalid flow_map IP address '<Address>' in '<LSP name>'	IP address is invalid.
	<Address>: Specified address <LSP name>: Specified LSP name
label_switched_path: invalid mask value '<value>' in 'to <Address>' not in 1 to 32 in '<LSP name>'	The masklen values for the "to parameters" are incorrect. Set the mask between 1 and 32.
	<value>: Specified mask length <Address>: Specified address <LSP name>: Specified LSP name
label_switched_path: invalid mask value '<Mask>' in '<LSP name>'	Mask value is invalid.
	<Mask>: Specified mask <LSP name>: Specified LSP name
label_switched_path: invalid mask value <Mask> in 'to <Address>' in '<LSP name>'	The masklen values for the "to parameters" are incorrect.
	<Mask>: Specified mask <Address>: Specified address <LSP name>: Specified LSP name
label_switched_path: invalid mask value at '<value>' not in 1 to 32 in '<LSP name>'	FLOW_MAP mask value is out of range. Set the mask between 1 and 32.
	<value>: Specified mask length <LSP name>: Specified LSP name
label_switched_path: invalid remote_vpn value at '<remote_vpnid>' not in range 1 to 1000000 in '<LSP name>'	Remote_vpn value is out of range. Specify a value within the range of 1 to 1000000
	<remote_vpnid>ÅFRemote vpn value <LSP name>: Specified LSP name
label_switched_path: invalid retry_interval value '<Seconds>' not in range 10 to 600 in '<LSP name>'	retry_interval value is out of range. Specify a value within the range of 10 to 600.
	<Seconds>: retry_interval value <LSP name>: Specified LSP name
label_switched_path: invalid 'to <Address>' in '<LSP name>'	The IP address for the "to parameters" is incorrect.
	<Address>: Specified address <LSP name>: Specified LSP name
label_switched_path: invalid vpn value at '<vpnid>' not in range 1 to 1000000 in '<LSP name>'	Vpn value is out of range. Specify a value within the range of 1 to 1000000
	<vpnid>: Specified vpn value <LSP name>: Specified LSP name
label_switched_path: last entry of explicit_routes must be same in '<LSP name>'	If "to" is not specified, the final entries to explicit_route used for label_switched_path and secondary_label_switched_path must agree with each other.
	<LSP name>: Specified LSP name

Downloaded from www.Manualslib.com manuals search engine

Table 5-10 MPLS Information Error Messages [ROUTE-OS7] (continued)

label_switched_path: the explicit_route_name '<ER name>' for the secondary_label_switched_path should not be the same explicit_route_name for the label_switched_path in '<LSP name>'	The name is incorrect. For lsp and secondary lsp, designate separate explicit_route_name.
	<ER name>: Specified route name <LSP name>: Specified LSP name
label_switched_path: vpn is necessary in '<LSP name>'	In setting remote_vpn, specify vpn.
	<LSP name>: Specified LSP name
label_switched_path: When VPN and flow_map are set up, ether one only a side is possible in '<LSP name>'	The flow_map and the vpn cannot be set simultaneously.
	<LSP name>: Specified LSP name
label_switched_path: When VPN and policy_mpls in flow block are set up, either one only a side is possible in '<LSP name>'	Simultaneous setting is not permitted for policy_mpls parameters of the flow filter and vpn parameters of label_switched_path. Do not specify LSP that uses VPN functions for a policy_mpls parameter of the flow filter. Also, do not make VPN settings for LSP that has been specified for a policy_mpls parameter of the flow filter.
	<LSP name>: Specified LSP name
label_switched_path:'<ER name>' is necessary	Unregistered explicit_route_name was designated. Or, an attempt was made to delete the explicit_route_name being used. Designate the registered explicit_route_name.
	<ER name>: Specified route name
ldp: Can not change IP address	IP address can not change.
ldp: duplicate failed_init_session_threshold	This is a duplicated definition.
ldp: duplicate keep_alive_hold_timer	This is a duplicated definition.
ldp: invalid failed_init value '<Value>' not in range 0 to 65535	failed_init is out of range. Specify a value within the range of 0 to 65535.
	<Value>: failed_init value
ldp: invalid IP address '<Address>'	IP address is invalid
	<Address>: Specified address
ldp: invalid keep_alive value '<HoldTimer>' not in range 1 to 65535	keep_alive value is out of range. Specify a value within the range of 1 to 65535.
	<HoldTimer>: HoldTimer value
ldp: ip address '<Address>' is already used in other ldp	Designate the IP address which has not been designated in the separate block.
	<Address>: Specified address
ldp: IP address is mandatory	The IP address is a must.
lsr: duplicate hop_count_limit	This is a duplicated definition.
lsr: duplicate loop_detection	This is a duplicated definition.
lsr: duplicate path_vector_limit	This is a duplicated definition.
lsr: invalid hop_count_limit value '<Value>' not in range 2 to 255	hop_count_limit value is out of range. Specify a value within the range of 2 to 255.
	<Value>
lsr: invalid path_vector_limit value '<Value>' not in range 2 to 255	path_vector_limit value is out of range. Specify a value within the range of 2 to 255.
	<Value>: path_vector_limit value
MPLS is not supported	MPLS is not supported
mpls syntax error	MPLS configuration information is invalid. Set the correct configuration information.
mpls: Can not change '<ER name>' with used	The "route name" whose route was tried to be changed is being used.
	<ER name>: Specified route name
mpls: Can not delete '<ER name>' with used	The "route name" whose route was tried to be deleted is being used.
	<ER name>: Specified route name
mpls: Can not set IPv6 IP_Address	It is not possible to set IPv6 addresses in MPLS information.

Downloaded from www.Manualslib.com manuals search engine

Table 5-10 MPLS Information Error Messages [ROUTE-OS7] (continued)

mpls: duplicate explicit_route_name '<ER name>'	The name is in existence. Use the explicit_name which is not used other blocks.
	<ER name>: Specified route name
mpls: duplicate label_switched_path_name '<LSP name>'	The name is in existence. Use the label_switched_path_name which is not used other blocks.
	<LSP name>: Specified LSP name
mpls: duplicate l2transport	Duplicate definitions.
mpls: duplicate lsp path to same destination '<address>'	The LSP to the same destination is in duplicated definition.
	<Address>: Specified address.
mpls: duplicate lsr	This is a duplicated definition.
mpls: duplicate platform_label_range	This is a duplicated definition.
mpls: duplicate topology_driven	This is a duplicated definition.
mpls: explicit_route is empty with used '<ER name>'	The empty explicit_route is used.
	<ER name>: Specified route name
mpls: interface not found at '<Interface Name>'	The specified interface does not exist. Set the interface name correctly.
	<Interface name>: Interface name
mpls: invalid platform_label_range value '<Label>' not in range 16 to 1048575	platform_label_range value is out of range. Specify label value within the range of 16 to 1048575.
	<Label>: Label value
mpls: invalid platform_label_range value '<Range>' not in range 16 to 1048575	platform_label_range value is out of range. Specify within the range of 16 to 1048575.
	<Range>: Range value
mpls: invalid vpn <VPN> IP configuration <Name>.	<VPN> of IP information <Name> is invalid. Set proper <VPN>.
	<Name> Name assigned to the configuration definition information
	<VPN> VPN defined in the configuration definition information
mpls: l2transport not specified '<Interface Name>'	The L2 transport is not set. Set the L2 transport in the line definition.
	<Interface name>: Interface name
mpls: No enough memory	Internal data memory supplement was failed.
mpls: number of CRLSP should be less than 256	The upper limit for CRLSP is 255.
mpls: range should not be less than label	platform_label_range value is invalid. For the “range”, set a value greater than that for the label.
mpls: The interface is neither ethernet nor gigabit_ethernet.	The specified interface is neither Ethernet nor gigabit Ethernet. Set an Ethernet or gigabit Ethernet interface.
mpls: too many MPLS definitions	The MPLS information has exceeded the maximum allowance.
Multcast and MPLS can not be set up simultaneously.	Multcast and MPLS can not be set up simultaneously
policy_mpls :' <LSP Name>' is invalid.	The name of LSP specified for a policy_mpls parameter of the flow filter must have been defined for label_switched_path. For the name of LSP specified for a policy_mpls parameter of the flow filter, use one already defined for label_switched_path. To delete from label_switched_path the name of LSP specified for a policy_mpls parameter of the flow filter, delete the policy_mpls parameter beforehand.
	<LSP name>: Specified LSP name
policy_mpls :' <LSP Name>' syntax error	The length of the LSP name specified for a policy_mpls parameter of the flow filter is illegal. For the name, use 1 to 14 characters.
	<LSP name>: Specified LSP name
secondary_label_switched_path: duplicate explicit_route_name in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name

Downloaded from www.Manualslib.com manuals search engine

Table 5-10 MPLS Information Error Messages [ROUTE-OS7] (continued)

secondary_label_switched_path: duplicate pinning in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
secondary_label_switched_path: duplicate retry_interval in '<LSP name>'	This is a duplicated definition.
	<LSP name>: Specified LSP name
secondary_label_switched_path: explicit_route_name is mandatory in '<LSP name>'	explicit_route_name is not specified. The explicit_route_name for the secondary_label_switched_path cannot be abbreviated.
	<LSP name>: Specified LSP name
secondary_label_switched_path: invalid retry_interval value '<Seconds>' not in range 10 to 600 in '<LSP name>'	retry_interval value is out of range. Specify a value within the range of 10 to 600.
	<Seconds>: retry_interval value <LSP name>: Specified LSP name
topology_driven: duplicate default	Default is a duplicated definition.
topology_driven: duplicate IP address in list at '<Address>'	IP address is a duplicated definition.
	<Address>: Specified address
topology_driven: duplicate retry_interval	This is a duplicated definition.
topology_driven: invalid retry_interval value '<Seconds>' not in range 10 to 600	The value for retry_interval is outside the range. Specify it with a value between 10 and 600.
	<Seconds>:retry_interval value
topology_driven: invalid IP address '<Address>'	IP address is a invalid.
	<Address>: Specified address

Downloaded from www.Manualslib.com manuals search engine

5.11 IPX Information

Table 5-11 IPX Information Error Messages

Message	Contents
Can not delete IPX with IPX filtering configuration.	Attempt made to delete a IPX where IPX filtering is set. After IPX filtering is deleted, delete IPX configuration.
Can not delete IPX with IPX interface configuration.	Attempt made to delete a IPX where IPX interface is set. After IPX interface is deleted, delete IPX configuration.
Can not delete IPX with IPX rip filtering configuration.	Attempt made to delete a IPX where rip filtering is set. After rip filtering is deleted, delete IPX configuration.
Can not delete IPX with IPX sap filtering configuration.	Attempt made to delete a IPX where sap filtering is set. After sap filtering is deleted, delete IPX configuration.
Can not delete IPX with IPX static route configuration.	Attempt made to delete a IPX where static route is set. After static route is deleted, delete IPX configuration.
Can not delete IPX with IPX static sap configuration.	Attempt made to delete a IPX where static sap is set. After static sap is deleted, delete IPX configuration.
Can not delete IPX with ipx-arp configuration.	Attempt made to delete a IPX where IPX ARP is set. After IPX ARP is deleted, delete IPX configuration.
Can not set ethernet-2.network address.	Ethernet-2.network address cannot be set. Ethernet-2.network address cannot be set on interface other than ethernet.
Can not set ethernet802.3 network address.	Ethernet802.3 network address cannot be set. Ethernet802.3 network address cannot be set on interface other than ethernet.
Can not set llc network address.	Network address cannot be set. Network address cannot be set on interface other than ether.
Can not set network address.	Llc network address cannot be set. Llc network address cannot be set on interface other than ether.
Can not set node address.	Node address cannot be set. Node address cannot be set on Ethernet interface.
Can not set snap network address.	Snap network address cannot be set. Snap network address cannot be set on interface other than ether.
Destination network not specified.	There is no setting of destination network number. Specify destination network number.
Destination Socket not specified.	There is no setting of destination socket address. Specify destination socket address.
Duplicate ethernet-2 network address, ethernet-2 network address.	Ethernet-2 network address and ethernet-2 network address are identical. Specify each ethernet-2 network address and ethernet-2 network address unique.
Duplicate ethernet-2 network address, ethernet802.3 network address.	Ethernet-2 network address and etherNet802.3 address are identical. Specify each ethernet-2 network address and etherNet802.3 address unique.
Duplicate ethernet-2 network address, llc network address.	Ethernet-2 network address and llc network address are identical. Specify each ethernet-2 network address and llc network address unique.
Duplicate ethernet-2 network address, network address.	Ethernet-2 network address and network address are identical. Specify each ethernet-2 network address and network address unique.
Duplicate ethernet-2 network address, snap network address.	Ethernet-2 network address and snap network address are identical. Specify each ethernet-2 network address and snap network address unique.
Duplicate ethernet802.3 network address, ethernet-2 network address.	Ethernet 802.3 network address and ethernet-2 network address are identical. Specify each ethernet 802.3 network address and ethernet-2 network address unique.
Duplicate ethernet802.3 network address, ethernet802.3 network address.	Ethernet 802.3 network address and ethernet 802.3network address are identical. Specify both of ethernet 802.3 network address unique.

Downloaded from www.Manualslib.com manuals search engine

Table 5-11 IPX Information Error Messages (continued)

Duplicate ethernet802.3 network address, llc network address.	Ethernet 802.3 network address and llc network address are identical. Specify each ethernet 802.3 network address and llc network address unique.
Duplicate ethernet802.3 network address, network address.	Ethernet 802.3 network address and network address are identical. Specify each ethernet 802.3 network address and network address unique.
Duplicate ethernet802.3 network address, snap network address.	Ethernet 802.3 network address and snap network address are identical. Specify each ethernet 802.3 network address and snap network address unique.
Duplicate IPX filtering.	Duplicate IPX filtering information is already specified. Specify all IPX filtering unique.
Duplicate IPX rip filtering.	Duplicate IPX rip filtering information is already specified. Specify all IPX rip filtering unique.
Duplicate IPX sap filtering.	Duplicate IPX sap filtering information is already specified. Specify all IPX sap filtering unique.
Duplicate IPX static route.	Duplicate IPX static route information is already specified. Specify all IPX static route unique.
Duplicate IPX static sap.	Duplicate IPX static sap information is already specified. Specify all IPX static sap unique.
Duplicate llc network address, ethernet-2 network address.	Llc network address and ethernet-2 network address are identical. Specify each llc network address and ethernet-2 network address unique.
Duplicate llc network address, ethernet802.3 network address.	Llc network address and ethernet802.3 network address are identical. Specify each llc network address and ethernet802.3 network address unique.
Duplicate llc network address, llc network address.	Llc network address and llc network address are identical. Specify each llc network address and llc network address unique.
Duplicate llc network address, network address.	Llc network address and network address are identical. Specify each llc network address and network address unique.
Duplicate llc network address, snap network address.	Llc network address and snap network address are identical. Specify each llc network address and snap network address unique.
Duplicate network address, ethernet-2 network address.	Network address and ethernet-2 network address are identical. Specify each network address and ethernet-2 network address unique.
Duplicate network address, ethernet802.3 network address.	Network address and ethernet802.3 network address are identical. Specify each network address and ethernet802.3 network address unique.
Duplicate network address, llc network address.	Network address and llc network address are identical. Specify each network address and llc network address unique.
Duplicate network address, network address.	Network address and network address are identical. Specify each network address and network address unique.
Duplicate network address, snap network address.	Network address and snap network address are identical. Specify each network address and snap network address unique.
Duplicate node address.	Duplicate node address is already specified. Specify each node address unique.
Duplicate snap network address, ethernet-2 network address.	Snap network address and ethernet-2 network address are identical. Specify each network address and ethernet-2 network address unique.
Duplicate snap network address, ethernet802.3 network address.	Snap network address and ethernet802.3network address are identical. Specify each network address and ethernet802.3network address unique.
Duplicate snap network address, llc network address.	Snap network address and llc network address are identical. Specify each network address and llc network address unique.
Duplicate snap network address, network address.	Snap network address and network address are identical. Specify each snap network address and network address unique.

Downloaded from www.Manualslib.com manuals search engine

Table 5-11 IPX Information Error Messages (continued)

Duplicate snap network address, snap network address.	Snap network address and snap network address are identical. Specify each snap network address and snap network address unique.
Hops not specified.	There is no setting of HOPS. Specify HOPS.
Interface name not specified.	Specified interface name not found. Enter a correct interface name.
Invalid name <name>.	Entered name of configuration information invalid. For IPX arp: Specify name set in dlci, vc and isdn ppp.
	A name of <name> configuration information.
IPX interface already defined.	Attempt to specify IPX interface in already defined. Specify correct interface
IPX not specified.	There is no setting of IPX. Specify IPX configuration.
Maximum number of IPX network addresses are already defined on the RP.	is already specification of valid number for IPX network per RP. Specify 32 addresses or less per RP.
Maximum number of IPX network addresses are already defined.	There is already specification of valid number for IPX network per router. Specify 160 addresses or less per router.
Next hop host not specified.	There is no setting of next hop host number. Specify next hop host number.
Network address not specified.	There is no specification of network address. Specify network address.
Network not specified.	There is no specification of forwarding network address. Specify forwarding network address.
Next hop network not specified.	There is no specification of next hop network. Specify next hop network number.
Next hop router address not specified.	There is no specification of next hop network address. Specify next hop network address.
No such insert index.	An entry cannot be inserted on specified entry number. Use entry number not exceeding the number of set entries.
No such set index.	An entry cannot be set on specified entry number. Use entry number not exceeding the set number of entries. To add entries, use the number of set entries +1 for entry value.
Node address not specified.	There is no specification of node address. Specify node address.
Protocol type not specified.	There is no specification of protocol type. Specify protocol type.
Server name not specified.	Server name is not specified. Specify server name.
Socket not specified.	There is no specification of forwarding socket address. Specify forwarding socket address.
Ticks not specified.	There is no setting of ticks. Specify ticks.
Type not specified.	There is no setting of types. Specify types.

Downloaded from www.Manualslib.com manuals search engine

5.12 Bridge Information

Table 5-12 Bridge Information Error Messages

Message	Contents
Action (drop , forward) not specified.	Action (drop, forward) not specified. Set drop or forward.
Duplicate extended filtering.	Duplicate extended filtering is set. Set the contents for all of the extended filtering information to unique.
Duplicate filtering database.	Duplicate filtering database is set. Set the contents for all of the filtering database information to unique.
Interface name not specified.	Specified interface name not found. Enter a correct interface name.
Invalid port mode.	Port mode is abnormal. Set to no for frame relay interface and DLCI group interface.
IP interface is not defined.	You are about to set the bridge interface for an interface without IP routing. Before setting the bridge interface, make settings for IP routing.
Length not specified.	Data length is not set. Specify the data length.
MAC address not specified.	MAC address is not set. Specify the MAC address.
Maximum number of bridge interfaces are already defined on the RP.	Maximum number of bridge interfaces are already defined on the RP. Set 32 or less interfaces per RP.
Maximum number of bridge interfaces are already defined.	Maximum number of bridge interfaces are already defined on the RP. Set 160 or less interfaces per router.
No such insert index.	An entry cannot be inserted on specified entry number. Use entry number not exceeding the number of set entries.
No such set index.	An entry cannot be set on specified entry number. Use entry number not exceeding the set number of entries. To add entries, use the number of set entries +1 for entry value.
Relations between forward delay time and max age time are inconsistent.	Relations between forward delay time and max age time are inconsistent. Set to meet 2 x (forward delay time -1) >= max age time.
Relations between max age time and hello time are inconsistent.	Relations between max age time and hello time are inconsistent. Set to meet max age time >= 2 x (hello time +1).

Downloaded from www.Manualslib.com manuals search engine

5.13 VRRP Information

Table 5-13 VRRP Information Error Messages

Message	Contents
Critical interface with target address not specified.	Critical interface is not set. Set critical interface in order to set target address.
Target address not specified.	Target address is not set. Set target address.
Failure detection times is greater than check trial times.	Failure detection times exceed check trial times. Set a value less than check trial times.
Recovery detection times is greater than check trial times.	Recovery detection times exceed check trial times. Set a value less than check trial times.
Check status interval is not in range of 1 to 255.	Check status interval exceeds the prescribed range. Set the value in the range of 1 - 255.
Check trial times is not in range of 1 to 10.	Check trial times exceeds the prescribed range. Set the value in the range of 1 - 10.
Failure detection times is not in range of 1 to 10.	Failure detection times exceeds the prescribed range. Set the value in the range of 1 - 10.
Failure detection interval is not in range of 1 to 255.	Failure detection interval exceeds the prescribed range. Set the value in the range of 1 - 255.
Recovery detection times is not in range of 1 to 10.	Recovery detection times exceeds the prescribed range. Set the value in the range of 1 - 10.
Recovery detection interval is not in range of 1 to 255.	Recovery detection interval exceeds the prescribed range. Set the value in the range of 1 - 255.

Downloaded from www.Manualslib.com manuals search engine

5.14 SNMP Information

Table 5-14 SNMP Information Error Messages

Message	Contents
Community name not specified.	Community name has not been specified. Specify community name.
Duplicate RMON alarm index.	The same alarm index is used. Make each alarm index unique.
Duplicate RMON event index.	The same event index is used. Make each event index unique.
Duplicate RMON history control index.	The same history control numbers are used. Make each history control number unique.
Duplicate snmp configuration.	Community name and manager IP address are the same. Change either to make each unique.
Invalid RMON history control line.	Specified line neither Ethernet nor Gigabit Ethernet. Specify Ethernet or Gigabit Ethernet line name.
Manager IP address not specified.	Manager IP address has not been specified. Specify manager IP address.
No such RMON history control line.	Specified line has not been set. Specify set Ethernet line name or Gigabit Ethernet line name.
RMON alarm falling event index not specified.	Falling event index has not been specified. Specify a falling event index.
RMON alarm falling threshold not specified.	Falling threshold has not been specified. Specify a falling threshold.
RMON alarm index not specified.	Alarm index has not been specified. Specify an alarm index.
RMON alarm interval not specified.	Threshold check interval has not been specified. Specify a threshold check interval.
RMON alarm rising event index not specified.	Rising event index has not been specified. Specify a rising event index.
RMON alarm rising threshold is less than falling threshold.	Rising threshold is less than the falling threshold. Increase the rising threshold no less than the falling threshold.
RMON alarm rising threshold not specified.	Rising threshold has not been specified. Specify a rising threshold.
RMON alarm sample type not specified.	Threshold check method has not been specified. Specify a threshold check method.
RMON alarm variable not specified.	Alarm MIB name has not been specified. Specify an alarm MIB name.
RMON event community not specified.	Trap community has not been specified. If event type is trap or log -trap, specify a trap community.
RMON event index not specified.	Event index has not been specified. Specify an event index.
RMON event type not specified.	Event type has not been specified. Specify an event type.
RMON history control index not specified.	History control number has not been specified. Specify a history control number.
RMON history control line name not specified.	Line name has not been specified. Specify a line name.

Downloaded from www.Manualslib.com manuals search engine

5.15 COPS Information

Table 5-15 COPS Information Error Messages

Message	Contents
Both are required for pepid and primary.	pepid and primary parameters are indispensable.
Both are required for server_password and cops_password.	Set both server_password and cops_password parameters when setting an encryption key.
COPS program is editing the configuration, please try again.	A COPS program is editing the configuration definition. Execute again after a little while.
COPS program is setting up policy, please try again.	A COPS program is setting a policy. Execute again after a little while.
cops_password is less than 64 characters.	The number of entered characters in a cops password parameter is out of the prescribed range. Set it using characters not exceeding 64.
Duplicate key id '<keyid>'	The same keyid cannot be set. Set different keyid.
	<Keyid>: Specified keyid.
illegal option -- <option>	Illegal option
	<option>: Specified option
pepid is less than 14 characters.	The number of entered characters in a pepid parameter is out of the prescribed range. Set it using characters not exceeding 14.
pepid is required.	A pepid parameter is indispensable.
primary is required.	A primary parameter is indispensable.
server_password is less than 64 characters.	The number of entered characters in a server_password parameter is out of the prescribed range. Set it using characters not exceeding 64.
The cops parameter of qos is required.	The cops parameter of a qos command is required when setting the COPS configuration definition.
The cops_range parameter of flow is required.	The cops_range parameter of a flow command is required when setting the COPS configuration definition.
The range of average_packet_size is 1024 - 65535.	The input value of an average_packet_size parameter is out of the prescribed range. Set it in the range of 1024 to 65535.
The range of backup_port is 0 - 65535.	The input value of a backup_port parameter is out of the prescribed range. Set it in the range of 0 to 65535.
The range of key id is 1 - 2147483647.	The number of entered characters in a keyid parameter is out of the prescribed range. Set it in the range of 1 to 2147483647.
The range of primary_port is 0 - 65535.	The input value of a primary_port parameter is out of the prescribed range. Set it in the range of 0 to 65535.
The range of retry_time is 0 - 10.	The input value of a retry_time parameter is out of the prescribed range. Set it in the range of 0 to 10.

Downloaded from www.Manualslib.com manuals search engine

5.16 RADIUS

Table 5-16 RADIUS Error Messages

Message	Contents
Range of retransmit is from 0 to 15.	The prescribed range for the "-retransmit" option is 0 - 15.
Range of timeout is from 1 to 30.	The prescribed range for the "-timeout" option is 1 - 30.
Range of auth_port is from 0 to 65535.	The prescribed range for the "-auth_port" option is 0 - 65535.
Parameter of key is wrong.	The secret key specified by the "-key" option is invalid. Use a maximum of 64 characters excluding prohibited characters.
key option required for server.	The "key" option must be set for each server.
Invalid IP address for server.	The server IP address is invalid.
Invalid hostname for server.	The server host name has a maximum of 255 characters.
The maximum number of server is 4.	It is not possible to specify more than 4 servers.
Configuration of server are duplicate.	An IP address with the same definition as an existing server setting has been specified.

Downloaded from www.Manualslib.com manuals search engine

5.17 Operation Management Information

Table 5-17 Operation Management Information Error Messages

Message	Contents
ntp: "<Address>" is not class D at multicastclient line	The specified address is not class D. Specify the correct address.
	<Address>: multicast address
ntp: "<Address>" not valid number at broadcast line	Invalid address is specified. Specify the correct address.
	<Address>: broadcast or multicast address
ntp: "<Address>" not valid number at peer line	Invalid address is specified. Specify the correct address.
	<Address>: peer address
ntp: "<Address>" not valid number at restrict line	Invalid address is specified. Specify the correct address.
	<Address>: restrict address
ntp: "<Address>" not valid number at server line	Invalid address is specified. Specify the correct address.
	<Address>: server address
ntp: broadcastdelay value <Value> is unlikely	The value specified to broadcastdelay is invalid. Specify fixed decimal less than 1.
	<Value>: broadcastdelay value.
ntp: broadcastdelay value <Value> un-decodable	The value specified to broadcastdelay is invalid. Specify fixed decimal less than 1.
	<Value>: broadcastdelay value
ntp: illegal value for clientlimit	The value specified to clientlimit is invalid. Specify a value from 1 to 4294967295.
ntp: inappropriate key number <Key> at authentication-key line	The specified key number is invalid. Specify a value from 1 to 4294967295.
	<Key>: key number
ntp: inappropriate key number <Key> at peer line	The specified key number is invalid. Specify a value from 1 to 4294967295.
	<Key>: key number
ntp: inappropriate key number <Key> at server line	The specified key number is invalid. Specify a value from 1 to 4294967295.
	<Key>: key number
ntp: inappropriate key value <Key> at authentication-key line	The specified key number is invalid. Specify a value from 1 to 4294967295.
	<Key>: key number
ntp: inappropriate stratum number <Value> at master line	The specified stratum value is invalid. Specify a value from 1 to 255.
	<Value>: stratum value
ntp: inappropriate version number <Version> at broadcast line	The specified version number is invalid. Specify a value from 1 to 3.
	<Version>: version number
ntp: inappropriate version number <Version> at peer line	The specified version number is invalid. Specify a value from 1 to 3.
	<Version>: version number
ntp: inappropriate version number <Version> at server line	The specified version number is invalid. Specify a value from 1 to 3.
	<Version>: version number
ntp: invalid mask "<Mask>" at restrict line	The specified netmask is invalid. Specify the correct netmask.
	<Mask>: mask value
ntp: master stratum value in error	The specified stratum value is invalid. Specify a value from 1 to 255.
ntp: specify parameter “-md5” at authentication-key line	Parameter -md5 is not specified. Specify parameter -md5.
ntp: too long keyword length at authentication-key line	The length of specified key word is too long. Specify 30 or less characters.
ntp: trusted key <Key> unlikely	The specified key number is invalid. Specify a value from 1 to 4294967295.
	<Key>: key number

Downloaded from www.Manualslib.com manuals search engine

5.18 Address Translation Information

Table 5-18 Address Translaion Information Error Messages

Message	Contents
nat:timeout is not in range 300 to 86400	The timeout value entered exceeds the prescribed range. Set it within the range of 300 - 86400.
nat:network mask length of NAT source IP address is not in range 8 to 32.	The post-conversion IP address mask length entered exceeds the prescribed range. Set it within the range of 8 - 32.
at:network mask length of NAT translation IP address is not in range 8 to 30 or 32.	The post-conversion IP address mask length entered exceeds the prescribed range. Set it within the range of 8 - 30 or 32.
nat:port is not in range 1 to 65535.	The port value entered exceeds the prescribed range. Set it within the range of 1 - 65535.
nat:port_range is not in range 1 to 65535.	The port_range value entered exceeds the prescribed range. Set it within the range of 1 - 65535.
nat:Invalid NAT source IP address.	The pre-translation IP address value entered is invalid. Set the IP address correctly.
nat:Invalid NAT translation IP address.	The post-translation IP address value entered is invalid. Set the IP address correctly.
nat:Invalid network mask length of NAT source IP address.	The pre-translation IP address mask length entered is invalid. Set mask length correctly.
nat:Invalid network mask length of NAT translation IP address.	The post-translation IP address mask length entered is invalid. Set mask length correctly.
nat:Invalid protocol.	The protocol value entered is invalid. Set protocol correctly.
nat:Invalid port.	The port value entered is invalid. Set port correctly.
nat:Invalid port_range.	The port_range value entered is invalid. Set port_range correctly.
nat:Invalid service.	The service value entered is invalid. Set service correctly.
nat:incorrect port_range parameters	The port number set behind the port_range range designation is smaller than the port number specified in front. Set port_range correctly.
nat:Maximum number of outside_interface are already defined.	Entries exceeding the maximum entry count of outside_interface are being added. Delete unnecessary entries before adding new entries.
nat:Maximum number of NAT rule are already defined.	Inbound NAT entries or outbound NAT entries exceeding the maximum entry count are being added to NAT rules. Delete unnecessary entries before adding new entries.
nat:illegal option -- protocol	"protocol" is an invalid option with the specified NAT type. Set the correct NAT type.
nat:illegal option -- port	"port" is an invalid option with the specified NAT type. Set the correct NAT type.
nat:illegal option -- port_range	"port_range" is an invalid option with the specified NAT type. Set the correct NAT type.
nat:illegal option -- service	"service" is an invalid option with the specified NAT type. Set the correct NAT type.
nat:No such name <name>.	The specified interface name does not exist. Set the correct interface name.
nat:Invalid name <name>.	The specified interface name is not valid as a NAT interface. Set the correct interface name.
nat:option requires an argument -- port	"Port" is an essential option with the specified NAT type. Set the "port" option.

Downloaded from www.Manualslib.com manuals search engine

Table 5-18 Address Translaion Information Error Messages (continued)

nat:option requires an argument -- service	"service" is an essential option with the specified NAT type. Set the "service" option.
nat:Can not specify "auto" to a source IP address.	It is not possible to specify pre-translation IP addresses as "auto" with the specified NAT type. Set the correct pre-translation IP address and mask length.
nat:Can not specify "auto" to a translation IP address.	It is not possible to specify post-translation IP addresses as "auto" with the specified NAT type. Set the correct pre-translation IP address and mask length.
nat:source: IP address must be network address,because network mask length is not 32.	The pre-translation IP address is not a network address for the specified mask length. Set the correct pre-translation IP address and mask length.
nat:translation: IP address must be network address,because network mask length is not 32.	The pre-translation IP address is not a network address for the specified mask length. Set the correct post-translation IP address and mask length.
nat:NAT translation IP address range over.	The post-translation IP address count of the specified range exceeds the maximum specifiable count of 1 rule. Set the correct post-translation IP address range.
nat:NAT translation IP address range count over.	The post-translation IP address count of the specified range exceeds the maximum specifiable count of 1 rule. Set the correct post-translation IP address range.
nat:Unmach NAT IP address count.	The pre-translation IP address count of the specified range does not coincide with the post-translation IP address count of the specified range in static NAT. Set the pre-translation IP address count of the specified range the same as the post-translation IP address count of the specified range.
Can not set nat configuration because qos_ip_list or filter_list configuration is already defined.	It is not possible to set nat configuration information because qos_ip_list or filter_list is set. It is necessary to delete "qos_ip_list" or "filter_list" in order to set nat.
Can not set nat because there are 2000 entries in all or more, nat configuration and flow configuration.	It is not possible to set nat configuration information because the total entry count of nat configuration information and flow configuration information that can be set per RP exceeds the RP settable entry count. Delete flow configuration information.
Can not set nat because nat reservation entry is used by flow configuration.	It is not possible to set nat configuration information because reserved entries of nat configuration information are being used by flow configuration information. Re-reflect configuration information by the "config copy" command in order to set nat configuration information.
Can not set nat configuration,qos_ip_list or filter_list configuration simultaneously.	It is not possible to simultaneously set nat configuration information and "qos_ip_list" or "filter_list" in configuration information files. Delete "qos_ip_list" or "filter_list" in order to set nat configuration information. Or, delete nat configuration information in order to set "qos_ip_list" or "filter_list."

Downloaded from www.Manualslib.com manuals search engine

5.19 DHCP Server Information

Table 5-19 DHCP Server Information Error Messages

Message	Contents
dhcp-server: expecting netmask	"Netmask" is not specified. Specify "netmask."
dhcp-server: fixed-address is already used	An IP address with the same "fixed address" is already in use. Specify a different IP address.
dhcp-server: interface not found at '<Interface Name>'	An interface with the specified interface name is not found. Specify it with a defined interface name.
dhcp-server: invalid DHCP option	This is an invalid DHCP option. Specify the correct DHCP option.
dhcp-server: invalid DHCP option value	This is an invalid DHCP option value. Set the correct setting value.
dhcp-server: invalid IP address	IP address is invalid. Set the correct IP address.
dhcp-server: invalid MAC address	This is an invalid MAC (hardware) address. Set the correct hardware address.
dhcp-server: invalid host-name	This is an invalid host name. Set the correct host name.
dhcp-server: invalid range	This is an invalid IP address range designation. Set the correct IP address range, checking the subnet and IP address range.
dhcp-server: invalid subnet address	This is an invalid subnet address designation. Specify the correct address.
dhcp-server: invalid time value	This is an invalid time designation. Specify the correct time.
dhcp-server: invalid value	This is an invalid value. Specify the correct value.
dhcp-server: it exceeded maximum number of IP-address pool	The value exceeds the maximum IP address pool value. Decrease the value the range definition of "dhcp subnet."
dhcp-server: maximum number of interfaces are already defined	Interfaces are being added that exceed the maximum interface count. Delete unneeded interfaces before adding new ones.
dhcp-server: no enough memory	The server is not operating due to insufficient memory. Decrease the DHCP server configuration definition.
dhcp-server: one or more than one interface definition are required to work a dhcp-server	One or more interfaces definitions are required for DHCP server operation. Define "dhcp interface."
dhcp-server: subnet conflicts	There is a subnet conflict. Enter the correct subnet to coincide with other subnet definitions.
dhcp-server: subnet definition which contains host IP address does not exist	A subnet definition that includes the host IP address does not exist. Define the subnet first.

Downloaded from www.Manualslib.com manuals search engine

5.20 DHCP Client Information

Table 5-20 DHCP Client Information Error Messages

Message	Contents
dhcp-client: maximum number of interfaces already defined	Interfaces are being added that exceed the maximum interface count. Delete unneeded interfaces before adding new ones.
dhcp-client: interface already used by other function	The specified interface is already in use by a function other than DHCP client.
dhcp-client: definition of IP address is not necessary for the interface used by DHCP client	An IP address definition is not required for the interface used by the DHCP client.
dhcp-client: interface not found at '<Interface Name>'	The specified interface does not exist. Set the correct interface name.
dhcp-client: invalid host-name	This is an invalid host name. Specify the correct host name.
dhcp-client: invalid dhcp-client-id-str	This is an invalid client ID. Specify the correct client ID.
dhcp-client: invalid DHCP option	This is an invalid DHCP option. Specify the correct DHCP option.

5.21 NAT-PT

Table 5-21 NAT-PT Error Messages

Message	Contents
illegal IP address format.	The IP address entry format is invalid.
illegal parameter.	The parameter is invalid.
Invalid NAT-PT prefix.	The NAT prefix is invalid. The following are possible reasons. 1. Host address is not 0. The length of the network prefix is 96 bits. Set the host address so that it is 0. 2. A link-local prefix has been set. It is not possible to set link-local prefixes. Set a different network prefix.
Invalid port range.	The post-translation port number range set by dynamic NAPT-PT translation rules is invalid. Set the first port number so that it is smaller than the last port number.
Natpt not specified.	The NAT-PT prefix is not set. Set a NAT-PT prefix first when setting NAT-PT information.
out of range.	The specified parameter exceeds the range. Set the value within the range.

Downloaded from www.Manualslib.com manuals search engine

5.22 DNS Resolver Information

Table 5-22 DNS Resolver Information Error Messages

Message	Contents
Can not set domain configuration without hostname configuration, or can not delete hostname configuration with domain configuration.	Add hostname configuration information before adding domain configuration information. Delete domain configuration information before deleting hostname configuration information.
Can not set domain configuration without nameserver configuration, or can not delete nameserver configuration with domain configuration.	Add nameserver configuration information before adding domain configuration information. Delete domain configuration information before deleting nameserver configuration information.
Can not set nameserver configuration without hostname configuration, or can not delete hostname configuration with nameserver configuration.	Add hostname configuration information before adding nameserver configuration information. Delete nameserver configuration information before deleting hostname configuration information.

5.23 Log Information

Table 5-23 Log Information Error Messages

Message	Contents
Can not set email configuration without smtp configuration, or can not delete smtp configuration with email configuration.	Add smtp configuration information before adding email configuration information. Delete email configuration information before deleting smtp configuration information.

5.24 E-Mail Sending Information

Table 5-24 E-Mail Sending Information Error Messages

Message	Contents
Can not set email configuration without email-from configuration, or can not delete email-from configuration with email configuration.	Add email-from configuration information before adding email configuration information. Delete email configuration information before deleting email-from configuration information.
Can not set email configuration without smtp configuration, or can not delete smtp configuration with email configuration.	Add smtp configuration information before adding email configuration information. Delete email configuration information before deleting smtp configuration information.

Downloaded from www.Manualslib.com manuals search engine

5.25 Other Error Messages

The following sub-commands (mainly, the open, close, save and copy sub-commands) are used for other purposes than for editing configuration definitions.

Table 5-25 Other Error Messages

Message	Contents
Bad address.	Access to MC card failed. Confirm setting status of MC card by using show mc command. When MC card is set correctly, wait for access, then execute again.
Cached configuration file is not created, current configuration file not be saved.	Because the contents of current configuration information file is not copied to temporarily saving configuration information file, current configuration information file is not saved. Eliminate the error and execute the command again. 1. Confirm the MC card's mounting status and the remaining capacity by using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2).
Can not execute config command in standby RM.	Config command unavailable in standby RM. Enter a config command in operation system.
CAUTION: Configuration file copy failed because cached configuration file create failed.	Because configuration file cannot be copied to cached configuration file, configuration file copy failed. Confirm setting status and the rest of memory size of MC card, and the execute again after eliminating causes of error.
CAUTION: Configuration file do not copy to standby RM because standby RM is not ready.	Standby configuration file copy failed. Confirm setting status and the rest memory size of standby MC card by using show mc command, and then execute the command again after eliminating causes of command.
CAUTION: Configuration file do not modified to standby RM because configuration file is opened in standby.	Because standby configuration information is opened, configuration file copy failed. Close standby configuration, and then execute the show mc command again.
CAUTION: Configuration file do not modified to standby RM because standby RM is not ready.	Because standby configuration information cannot be modified, configuration file copy failed. Confirm status and operation of the standby, and then execute the command again.
CAUTION: Current configuration file was successfully changed. Configuration file do not modified to standby RM because standby RM is not ready.	Current configuration file was copied, but because standby configuration information cannot be modified, standby configuration information is not reflected. When updating standby configuration file, confirm status and operation of standby, and then reflect by using config copy command. 1. Confirm the MC card's mounting status and the remaining capacity in the standby system using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2). 3. Confirm that the standby system RM board has been inserted into this device correctly.
CAUTION: Current configuration file was successfu11y changed. Configuration file do not modified to stand by RM because cached configuration file create failed.	Current configuration file was copied, but because standby configuration information cannot be copied to cached configuration file, standby configuration information is not reflected. When updating standby configuration file, Confirm setting status and the rest memory size of standby MC card by using show mc command, and then reflect by using config copy command after eliminating causes of error.
CAUTION: Current configuration file was successfully changed. Configuration file did not copy to standby RM because standby RM is not ready.	Current configuration file was copied, but because standby RM is not ready, standby configuration file copy failed. When updating standby configuration file, reflect after starting up standby by using config copy.

Downloaded from www.Manualslib.com manuals search engine

Table 5-25 Other Error Messages (continued)

CAUTION: Current configuration file was successfully changed. Configuration file do not modified to standby RM because configuration file copy failed.	Current configuration file was copied, but because it cannot be copied to standby configuration file, standby configuration information is not reflected. When updating standby configuration file, reflect by using config copy command after eliminating causes of error. 1. Confirm the MC card's mounting status and the remaining capacity in the standby system using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2). 3. Confirm that the standby system RM board has been inserted into this device correctly.
CAUTION: Current configuration file was successfully saved. Update configuration file do not copy to standby RM because standby RM is not ready.	Current configuration file was saved, but because standby RM is not ready, standby configuration information is not reflected. When updating standby configuration information, start up the standby, and then reflect by using config copy command.
CAUTION: Current configuration file was successfully saved. Update configuration file do not modified to standby RM because configuration file copy failed.	Current configuration file was saved, but because it cannot be copied to standby configuration file, standby configuration information is not reflected. When updating standby configuration file, reflect by using config copy command after eliminating causes of error. 1. Confirm the MC card's mounting status and the remaining capacity in the standby system using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2). 3. Confirm that the standby system RM board has been inserted into this device correctly.
CAUTION: Current configuration file was successfully saved. Update configuration file do not modified to standby RM because configuration file is opened in standby RM.	Current configuration file was saved, but because standby configuration information is opened, standby configuration information is not reflected. When updating configuration information, close standby configuration, and then reflect by using config copy command.
CAUTION: Current configuration file was successfully saved. Update Configuration file do not modified to stand by RM because stand by RM is not ready.	Current configuration information file was copied, but because standby configuration file cannot be modified, standby configuration information is not reflected. When updating standby configuration file, reflect by using config copy command after eliminating causes of error. 1. Confirm the MC card's mounting status and the remaining capacity in the standby system using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2). 3. Confirm that the standby system RM board has been inserted into this device correctly.
CAUTION: Current configuration file was successfully saved.Update configuration file do not modified to standby RM because cached configuration file create failed.	Current configuration file was saved, but because standby configuration information cannot be copied to cached configuration file, standby configuration information is not reflected. When updating configuration information, confirm the rest memory size of MC card by using show mc command, and then reflect by using config copy command after eliminating causes of error.
CAUTION: Current configuration file was successfully changed. Configuration file was not modified to standby RM because configuration file is opened in standby RM.	Current configuration file was copied, but because standby configuration information is opened, standby configuration information is not reflected. When updating standby configuration file, close standby configuration, and then reflect by using config copy command.
Command incomplete because processing configuration deletion exceeded time limit. To complete deletion, please try same command again.	Because processing deletion of configuration is taking too much time, command is interrupted. Execute same command again.
Configuration file can not open.	Configuration file cannot open. Confirm setting status and the rest memory size of MC card by using show mc command.

Downloaded from www.Manualslib.com manuals search engine

Table 5-25 Other Error Messages (continued)

Configuration file copy failed.	Configuration file copy failed. Execute the command again after removing the factors causing the following errors. 1. Confirm the MC card's mounting status and the remaining capacity in the standby system using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2).
Configuration file copy failed because cached configuration file create failed.	Because configuration file cannot be copied to cached configuration file, configuration file copy is failed. Execute the command again after removing the factors causing the following errors. 1. Confirm the MC card's mounting status and the remaining capacity in the standby system using the show mc command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2).
Configuration file do not copy to standby RM because standby RM is not ready.	Standby configuration file copy failed. Confirm setting information and the rest memory size of standby MC card using the show mc command, and then execute again after eliminating causes of error.
Configuration file do not modified to standby RM because configuration file is opened in standby RM.	Because standby configuration information is opened, configuration file copy failed. Close standby configuration, and then execute the command again.
Configuration file do not modified to standby RM because standby RM is not ready.	Because standby configuration information cannot be modified, configuration file copy failed. Eliminate the error and execute the command again. 1. Confirm the standby MC card's mounting status and the remaining capacity in the standby system using the "show me" command (*1). 2. Confirm the RM's CPU use rate using the show "rm cpu" command (*2). 3. Confirm that the standby system RM board has been inserted into this device correctly.
Configuration file is already closed.	Current or spare configuration file already closed. Before entering configuration information, open current or spare configuration file.
Configuration file is already opened, configuration file did not copy.	Current or spare configuration file already opened. Command could not be executed successfully. Before entering configuration information, close current or spare configuration file.
Configuration file is already opened.	Current or spare configuration file already opened. Close current or spare configuration file.
Configuration file not found.	Target current or spare configuration file not found. Specify correct current or spare configuration file and execute again.
Configuration file save error.	Current or spare configuration file cannot be saved. Using the show mc command, check the installation status of the MC card, remaining MC card memory and other statuses.
Current configuration file was successfully changed. Configuration file do not copy to standby RM because standby RM is not ready.	Current configuration information file was copied, but because standby RM is not started up, standby configuration information is not copied. When updating standby configuration file, start up standby and reflect by using config copy command.
Current configuration file was successfully changed. Configuration file do not modified to standby RM because cached configuration file create failed.	Current configuration information file was copied, but because standby configuration information cannot be copied to cached configuration file, standby configuration information is not reflect. When updating standby configuration file, confirm the rest memory size of MC card by using show mc command, and then reflect by using config command after eliminating causes of error.
Current configuration file was successfully changed. Configuration file do not modified to standby RM because configuration file copy failed.	Current configuration information file was copied, but because current configuration file cannot be copied to standby configuration file, standby configuration information is not reflected. When updating standby configuration file, confirm setting status and the rest memory size of MC card by using show mc command, and then reflect by using config command after eliminating causes of error.

Downloaded from www.Manualslib.com manuals search engine

Table 5-25 Other Error Messages (continued)

Current configuration file was successfully changed. Configuration file do not modified to standby RM because configuration file is opened in standby RM.	Current configuration information file was copied, but because standby configuration file is opened, standby configuration information is not reflected. When updating standby configuration information, close standby configuration, and then use config copy command.
Current configuration file was successfully changed. Configuration file do not modified to standby RM because standby RM is not ready.	Current configuration information file was copied, but because standby configuration file cannot be modified, standby configuration information is not reflected. When updating standby configuration information, confirm standby status and operation, and then reflect standby configuration information by using config command.
Current configuration file was successfully saved. Update configuration file do not copy to standby RM because standby RM is not ready.	Current configuration information file was saved, but because standby RM is not setup, standby configuration information is not reflected. When updating standby configuration information, use copy command after setup the standby.
Current configuration file was successfully saved. Update configuration file do not modified to standby RM because cached configuration file create failed.	Current configuration information file was saved, but because standby configuration information cannot be copied to cached configuration file, standby configuration information is not reflected. When updating standby configuration information, confirm the rest memory size of standby MC card by using show mc command, and reflect standby configuration information by using copy command after eliminating causes of error.
Current configuration file was successfully saved. Update configuration file do not modified to standby RM because configuration file copy failed.	Current configuration information file was saved, but because this current configuration file cannot be copied to standby configuration information file, standby configuration information is not reflected. When updating standby configuration information, confirm setting status and the rest memory size of standby MC card by using show mc command, and reflect standby configuration information by using copy command after eliminating causes of error.
Current configuration file was successfully saved. Update configuration file do not modified to standby RM because configuration file is opened in standby RM.	Current configuration information file was saved, but because standby configuration file is opened, standby configuration information is not reflected. When updating standby configuration information, close standby configuration, and then use config copy command.
Current configuration file was successfully saved. Update Configuration file do not modified to standby RM because standby RM is not ready.	Current configuration information file was saved, but because standby configuration file cannot be modified, standby configuration information is not reflected. When updating standby configuration information, confirm standby status and operation, and then reflect standby configuration information by using config command.
Device out of space.	Because the memory of MC card running short, data can not be saved to specified file. Delete unnecessary file of MC card.
File exists.	Specified file name can not be used. Specify another file name.
Filename or directory path is too long.	The spare configuration filename or directory path exceeds 256 characters. Shorten the spare configuration filename or directory path.
Input/output error.	Access to MC card failed. Confirm setting status of MC card by using show mc command. When MC card is set correctly, wait for access, then execute again.
Is a directory.	Because specified file name is directory, it can not be used. Enter a correct file name.
Not enough memory, configuration file is too big.	Because current or spare configuration file is too big, memory size is insufficient. Using the editor, delete unnecessary definitions in the configuration definition information file. Confirm RM memory using the "show router" command (*3) and, if RM memory is less than 256Mb, increase it to 256Mb or more and then edit the configuration information again.
No such file or directory.	Specified file or directory not exist. Enter correct file name or directory.

Downloaded from www.Manualslib.com manuals search engine

Table 5-25 Other Error Messages (continued)

Not a directory.	Specified file name invalid. Enter a correct file name.
Operation not permitted.	Because operation configuration information written in memory is being edited, operation is not permitted.
Permission denied.	Permission denied. Specified file can not be accessed. Release access control for file or directory by using Operations Guide -New Syntax Operation Command, Vol. 1- chmod command.
Resource temporarily unavailable.	System resource running short. Wait for access, then execute again.
syntax error line <Line No.>	One of the following problems may occur regarding the configuration information of <Line No.>. Define the correct configuration information. 1. The syntax or the range of values is invalid. Define the correct syntax or value. 2. The maximum definable entry count is exceeded. Define the value within the set range. 3. The required configuration information has not been defined. Define the lacking configuration information. 4. The same configuration information has been defined more than once. Deleted unneeded configuration information.
Text file busy.	Unavailable access to specified file. Wait for access, then execute again.
Too many levels of symbolic links.	Specified file can not be detected. Decrease symbolic links.
Too many open files in system.	System resource running short. Wait for access, then execute again.

**1: Refer to* GR2000 Operations Commands, Vol. 1 *for* show mc *command.*
**2: Refer to* GR2000 Operations Commands, Vol. 1 *for* show rm cpu *command.*
**3: Refer to* GR2000 Operations Commands, Vol. 1 *for* show router *command.*

Downloaded from www.Manualslib.com manuals search engine

Index

A

alarm, snmp object 3-12
alarm-group information 3-12
ARP info. when WAN (frame relay) is used 2-9

B

board disablement object --- disable 4-31
bridge 2-29
bridge objects 2-29
    bridge 2-29
    bridge-interface 2-30
    extended-filtering 2-35
    filtering-database 2-33
    spanning-tree 2-39
bridge-interface 2-30

C

command
    bridge 2-29
    snmp 3-1
community 3-19
community name 3-2
config
    default 4-33

D

default 4-33
default config object
    default 4-33
    router-default 4-60
default configuration objects 4-33
default, router 4-60
description 3-20
discard mode, QoS 1-166
dns-resolver 4-3

E

e-mail, log info. 4-9, 4-11
event 3-19
event, SNMP object 3-19
extended-filtering 2-35

F

falling_event 3-14
falling_threshold 3-14
FDB (filtering-database) 2-33
filter 1-108
filter-group 1-124
filtering-database 2-33
filter-interface 1-128
filter-list 1-110
flow control
    IPv4
        IPv6 1-2
flow information 1-2, 1-9
flow, qos 1-57
flow-control parameters, IP QoS 1-169

H

HDLC passthrough QoS settings 1-209
history-control, snmp object 3-8
host name information 4-1
    dns-resolver 4-3
    hosts 4-1
hosts 4-1

I

IGMP
    type number, filter-list 1-119
index 3-8, 3-12, 3-19
interface names, QoS 1-155
interval 3-9, 3-13
IP frames, QoS conditions 1-168
IP informational object
    filter 1-108
    filter-group 1-124
    filter-interface 1-128
    filter-list 1-110
IP QoS information control, range of 1-133
IP QoS settings 1-201
IPX 2-1
IPX objects 2-1
    ipx-arp 2-9
    ipx-filtering 2-24
    ipx-interface 2-3
    rip-filtering 2-18
    sap-filtering 2-21

Downloaded from www.Manualslib.com manuals search engine

static-route 2-11
static-sap 2-14
IPX QoS settings 1-205
IPX routing protocol info. 2-1
IPX static route settings 2-11
ipx-arp 2-9
ipx-filtering 2-24
ipx-interface 2-3

L

line
name 3-8
log information 4-7
logger-email 4-9, 4-11
logger-smtp 4-12
logger-syslog 4-7
logger-email 4-9, 4-11
logger-smtp 4-12
logger-syslog 4-7

N

NIF, disabled 4-31
none | -trap | -ex_trap 3-2
NTP Object --- ntp 4-20

O

owner 3-9, 3-14, 3-20

P

pair switch 1-117
parameter
ageing 2-33
branch 1-119
community 3-19
community name 3-2
description 3-20
falling_event 3-14
falling_threshold 3-14
hops 2-15
icmp_type 1-118
igmp_type 1-119
index 3-8, 3-12, 3-19
interval 3-9, 3-13
line name 3-8
MAC Address 2-34
max_age_time 2-39
none|-trap 3-2
owner 3-9, 3-14, 3-20
policy_routing 1-119
read 3-2
replace_tos 1-120
rising_event 3-13
sample 3-13
snmp manager ip address 3-2
startup 3-13
type 3-19
variable 3-12

Q

QoS 1-131, 1-134
attribute, range of 1-131
discard mode control, range of 1-132
info., control range 1-131
interface control, range of 1-131
interface names 1-155
IP frame condition group info., range of 1-133
IP frame condition group settings 1-194
IP frame condition info., range of 1-133
mode (priority, round-robin, or bandwidth), qos-queue-list 1-138
settings 1-207
QoS flow information 1-57
qos-bridge 1-207
qos-discard-mode 1-166
qos-hdlc-passthrough 1-209
qos-interface 1-153
qos-ip 1-201
qos-ip-list 1-168
qos-ip-list-group 1-194
qos-ipx 1-205
qos-queue-list 1-138
qos-tos-map 1-196
quality of service (QoS) object 1-205
QoS 1-134
qos-bridge 1-207
qos-discard-mode 1-166
qos-hdlc-passthrough 1-209
qos-interface 1-153
qos-ip 1-201
qos-ip-list 1-168
qos-ip-list-group 1-194
qos-queue-list 1-138
qos-tos-map 1-196
quality of service (QoS) objects 1-131

R

read | -read_write 3-2
rip-filtering 2-18
rising_event_index 3-13
RMON (RFC1757) ethernet
alarm-group info. 3-12
event-group info. 3-19
RMON, SNMP objects 3-1
router-default, default config. objects 4-60

Downloaded from www.Manualslib.com manuals search engine

S

sample 3-13
sap-filtering 2-21
show, subcommand 4-34, 4-40, 4-42, 4-43, 4-46, 4-48, 4-50, 4-51, 4-54, 4-56, 4-57, 4-59
SNMP
    information objects, application of 3-1
snmp 3-1
SNMP manager IP Address 3-2
SNMP managers
    creation 3-1
    deletion 3-1
    display 3-1
    modification 3-1
SNMP object
    alarm 3-12
    event 3-19
    history-control 3-8
SNMP objects 3-1
spanning-tree 2-39
startup_alarm 3-13
static-route 2-11
static-sap 2-14
subcommand
    show 4-34, 4-40, 4-42, 4-43, 4-46, 4-48, 4-50, 4-51, 4-54, 4-56, 4-57, 4-59
syslog interface, log info. 4-7

T

tos , filter-list 1-112
tos-qos conversion table info. control, range of 1-134
trap system message levels 3-3
type 3-19

V

variable 3-12

Downloaded from www.Manualslib.com manuals search engine

Hitachi Gigabit Router GR2000 Series Enhanced Version Configuration Commands, Vol. 2, Part No. GR2K-GA-0014, Version 07-02
Copyright © 2002, Hitachi America, Ltd., All rights reserved, Printed in the U.S.A.
Hitachi America, Ltd., 2000 Sierra Point Parkway, Brisbane, CA 94005-1835 U.S.A.

Downloaded from www.Manualslib.com manuals search engine